Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 9

Information Security Law in the EU and the U.S. – A Risk-Based Assessment of Regulatory Policies

Lukas Feiler

2011

TTLF Working Papers

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

Sponsors

This project was co-sponsored by the Stanford-Vienna Transatlantic Technology Law Forum (Stanford Law School/University of Vienna School of Law), the Stanford Center for E-Commerce, the Europe Center at the Freeman Spogli Institute for International Studies at Stanford University, as well as supported by the University of Vienna Research Grant 2010.

About the Author

Lukas Feiler is an associate at Wolf Theiss Attorneys at Law, Vienna. He earned his law degree from the University of Vienna School of Law in 2008 and a Systems Security Certified Practitioner (SSCP) certification from (ISC)^2 in 2009. He also studied U.S. cyberspace law and intellectual property law at Santa Clara University. Previous activities include a position of Vice Director at the European Center for E-Commerce and Internet Law, Vienna (2005-2011), a traineeship with the European Commission, DG Information Society & Media, Unit A.3 "Internet; Network and Information Security" in Brussels (2009), software developer positions with software companies in Vienna, Leeds, and New York (2000-2011), and a teaching position for TCP/IP networking and web application development at the SAE Institute Vienna (2002-2006). He is the co-author of three books, the author of numerous law review articles published *inter alia* in the Santa Clara Computer & High Technology Law Journal, the European Journal of Law and Technology, and the Computer Law Review International, and lead developer of the open source project Query2XML, which was accepted for inclusion in the official PHP Extension and Application Repository. He has been a TTLF Fellow since August 2009 and a Europe Center Research Affiliate since November 2009.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project

Suggested Citation

This TTLF Working Paper should be cited as:
Lukas Feiler, Information Security Law in the EU and the U.S. – A Risk-Based Assessment of Regulatory Policies, TTLF Working Paper No. 9, http://www.law.stanford.edu/program/centers/ttlf/papers/feiler_wp9.pdf.

Copyright

Abstract

The advancement and proliferation of information technology has led to a drastic increase of the amount of personal and non-personal information that is being stored, processed, or transmitted by individuals, businesses, and governments. These developments have increased the need for effective information security—i.e. the preservation of confidentiality, integrity, and availability of information. Since private as well as governmental actors continue to fail to provide an adequate level of information security, policy makers (legislators, judges, and regulators) were prompted to formulate regulatory policies that explicitly address the issue of information security.

This paper identifies, analyses, and comparatively assesses regulatory policies in EU and U.S. law which address information security. As regards U.S. law, the paper discusses federal law as well as the law of the States of California and New York.

The assessed policies typically take one of the following forms: First, they may require the implementation safeguards, whether for publicly traded companies, service providers, government authorities, software manufacturers, or organizations which handle personal information. Second, they may impose or limit liability in particular as regards software manufacturers, service providers, payment service providers, payment service users, or entities that are responsible for the processing of personal information. Third, policies addressing information security may mandate transparency, in particular by requiring the notification of breaches of information security or breaches of network security, mandating the disclosure of vulnerabilities by publicly traded companies, or prohibiting deceptive security claims about products and services. Fourth, such policies may attempt to deter malicious actors from mounting any threats against the security of information, in particular by providing criminal sanctions.

To aid this comparative assessment, a risk-based assessment methodology is developed which is based on different risk treatment options. The paper also contains a concluding comparative assessment that summarizes the current state of information security regulation in the EU and the U.S. This concluding assessment highlights the extent to which current regulatory policies make use of the available risk treatment options, which actors of the information security landscape receive the most regulatory attention and which are more or less ignored, as well as whether the current regulatory policies are suitable to address the fundamental challenges of information security.

Building on this concluding assessment, policy recommendations equally applicable to the EU and the U.S. are presented. The paper does not propose the adoption of a single radical measure but rather a holistic web of balanced measures that in concert may have the potential to fundamentally improve information security.

Contents—Summary

Contents

1. Introduction

For the purpose of this thesis, “information security” is defined as the preservation of confidentiality, integrity, and availability of information that has value to an organization or an individual.[1] The term “information security” is closely related to the term “data security” (sometimes also referred to as “IT security”). Information security has a broader scope as it is also concerned with information that exists in non-electronic form. However, this distinction is less important than it might seem. Most information is actually stored, processed, and transmitted in electronic form anyway. Information security, to a large extent, therefore is congruent with IT security.

The advancement and proliferation of information technology has led to a drastic increase of the amount of information that is being preserved. Due to the low cost of data storage and data processing, information that used to be discarded immediately after its creation (e.g. what goods a certain customer bought in the supermarket, which books he read or where he drove his car), is now being retained for long periods of time. These developments have made our society more vulnerable and therefore more dependent on information security. Depending on the nature of the information, we most value its confidentiality (e.g. our medical records), its integrity (e.g. a database of outstanding arrest warrants), or its availability (e.g. our medical records in emergency cases). However, man-made threats like viruses,[2] worms,[3] social

[1] *See infra* chapter 2.1 (further elaborating on this definition).

[2] *See infra* chapter 3.1 (discussing various forms of malicious software).

[3] *See id*.

engineering,[4] or simple human error as well as natural threats like fire, floods, or earthquakes pose serious risks for information assets.

Many governmental and private actors continue to fail to provide an adequate level of information security. This has prompted policy makers (legislators, judges, and regulators) to formulate regulatory policies that explicitly address the issue of information security.

Any fruitful discussion on regulatory policies necessarily centers on the issue of how they affect information security. This raises the question of how to express varying levels of information security. It has long been accepted that information security is not a matter of "secure" or "unsecure", but rather a matter of degree that is best expressed in terms of risk. Information security risk is defined, for the purpose of this thesis, as the probability that a threat agent will give rise to a threat that exploits a vulnerability of an information asset, circumvents potential safeguards and thereby causes harm to an organization or an individual.[5]

The object of study is, firstly, the identification and analysis of regulatory policies in EU and U.S. law which address information security. Secondly, a risk-based methodology for the assessment of the policies is developed. Thirdly, that methodology is used to perform a risk-based assessment of the identified regulatory policies.

When analyzing U.S. law, the thesis will discuss federal law as well as state law. However, due to the economic importance of the states of California and New York, these jurisdictions will be the exclusive focus of the state law analysis.

[4] *See infra* chapter 2.4.2 (discussing the nature of social engineering).

[5] *See infra* chapter 3.1 (further elaborating on this definition).

Previous works with a similar object of study were either limited to general discussions of U.S. law without providing an assessment of the law's effectiveness,[6] have only analyzed the law of a single EU Member State without providing a comparison with the law of another jurisdiction,[7] or have approached information security regulation primarily from an economic instead of a legal perspective.[8]

With the continuous advancement and proliferation of information technology, information security will continue to grow in importance not only for organizations, the economy, and the society as a whole but also for individuals. From medical and criminal records to credit histories, individuals are more and more dependent on centrally stored information. With this increased importance comes the risk of reacting emotionally to information security issues. A lack of technical understanding in the general public and overstated threats like "cyber terrorism"[9] or "cyber war"[10] particularly increase the incentives for policy makers to create regulatory policies that give people a feeling of improved security while doing little or

[6] *See* MARK G. MILONE, INFORMATION SECURITY LAW: CONTROL OF DIGITAL ASSETS (2009); ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL, STATE AND INTERNATIONAL LAW (2009).

[7] *See* GERALD SPINDLER ET AL., VERANTWORTLICHKEITEN VON IT-HERSTELLERN, NUTZERN UND INTERMEDIÄREN [RESPONSIBILITIES OF IT MANUFACTURERS, USERS, AND INTERMEDIARIES] (2007), *available at* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf?__ blob=publicationFile (discussing the liability of IT manufacturers, users, and intermediaries under German law).

[8] *See* ROSS ANDERSON ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport (making policy recommendations, based on economic principles and empirical data, for how to address information security issues in the EU).

[9] *See infra* chapter 2.3.7 (briefly discussing the risk of "cyber terrorism").

[10] *Cf.* PETER SOMMER & IAN BROWN, ORG. FOR ECON. CO-OPERATION AND DEV. [OECD], REDUCING SYSTEMIC CYBERSECURITY RISK, IFP/WKP/FGS(2011)3, at 7 (2011), *available at* http://www.oecd.org/dataoecd/3/42/ 46894657.pdf (noting that the "[a]nalysis of cybsersecurity issues has been weakened by […] the use of exaggerated language" such as by referring to cyberespionage activities as "few keystrokes away from cyberwar").

nothing to actually improve security (a pattern generally referred to as “security theatre”).[11] Objective approaches are needed to allow for a productive discussion on regulatory policies affecting information security, thus eventually leading to higher levels of information security, from which all stand to benefit.

The objective of this thesis is to scientifically assess different regulatory policy options using a risk-based methodology, thereby helping to focus on real information security improvements as opposed to “security theater.”

[11] *See* Bruce Schneier, *Beyond Security Theater*, NEW INTERNATIONALIST, Nov. 2009, at 10, *available at* http://www.schneier.com/essay-292.html.

2. The Foundations and Challenges of Information Security

2.1. Information Security Defined

Following international standards, *information security* is defined here as the preservation of confidentiality, integrity, and availability of knowledge or data[12] that has value to an organization or an individual.[13] The concepts of information confidentiality, integrity, and availability are therefore of central importance.[14]

Confidentiality is defined as the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.[15] *Integrity* is defined as the protection of accuracy and completeness of information.[16] *Availability* is the property of being accessible

[12] Within this thesis, "data" is treated as a mass noun. *Cf.* http://www.computer.org/portal/web/publications/styleguidedef (last accessed Feb. 10, 2011; stating that, according to the IEEE Computer Society Style Guide, the author should follow his own preference for use as singular or plural).

[13] *See* INT'L ORG. FOR STANDARDIZATION [ISO] & INT'L ELECTROTECHNICAL COMM'N [IEC], INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.18 (2009) (defining "information security" as the "preservation of confidentiality, integrity and availability of information). *See id.* § 2.19 (defining "information asset" as "knowledge or data that has value to the organization").

[14] *Cf.* Todd Fitzgerald et al., *Information Security and Risk Management, in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 1, 5 (Harold F. Tipton ed., 2007) (identifying confidentiality, integrity, and availability as the "Core Information Security Principles"); SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 59 (4th ed. 2008) (stating that information security programs have three main principles: availability, integrity, and confidentiality).

[15] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.9 (2009). *Cf.* Federal Information Security Management Act of 2002 § 301, 44 U.S.C. § 3542(b)(1)(B) (defining "confidentiality" as "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information"); Parliament and Council Regulation 460/2004, art. 4(g), 2004 O.J. (L 77) 1, 5 (EC) (defining "data confidentiality" as "the protection of communications or stored data against interception and reading by unauthorised persons").

[16] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.25 (2009). *Cf.* Federal Information Security Management Act of 2002 § 301, 44 U.S.C. § 3542(b)(1)(A) (defining "integrity" as "guarding against improper information modification or destruction […]"); Parliament and Council Regulation 460/2004, art. 4(f), 2004 O.J. (L 77) 1, 5 (EC) (defining "data integrity" as "the confirmation that data which has been sent, received, or stored are complete and unchanged").

and usable upon demand by an authorized entity[17] and is often expressed as a function of Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR).[18] While laypeople may not consider (temporary) unavailability a security concern, the information security profession rightly treats it as such because the unavailability of information can have equally drastic consequences as a loss of confidentiality or integrity[19] (e.g. in the case of medical information in an emergency situation).

It has to be noted that threats to the confidentiality, integrity, and availability of information do not only originate from (cyber) criminals but from a wide range of sources, including humans acting by mistake and natural disasters.[20]

[17] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.7 (2009). *Cf.* Federal Information Security Management Act of 2002 § 301, 44 U.S.C. § 3542(b)(1)(C) (defining "availability" as "ensuring timely and reliable access to and use of information"); Parliament and Council Regulation 460/2004, art. 4(d), 2004 O.J. (L 77) 1, 5 (EC) (stating "availability" means "that data is accessible and services are operational").

[18] *See, e.g.,* CHRIS OGGERINO, HIGH AVAILABILITY NETWORK FUNDAMENTALS 12 (2001); EVAN MARCUS & HAL STERN, BLUEPRINTS FOR HIGH AVAILABILITY 17 (2003); DODDERI NARSHIMA PRABHAKAR MURTHY ET AL., PRODUCT RELIABILITY: SPECIFICATION AND PERFORMANCE 80 (2008). *Cf.* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 1057 et seq. (4th ed. 2008) (defining "MTBF" as "the estimated lifespan of a piece of equipment" and "MTTR" as "the amount of time it will be expected to take to get a device fixed and back into production"). Note that availability as defined above is sometimes also referred to as "operational availability." It has to be contrasted with inherent (or intrinsic) availability which is not directly relevant for information security since it is a function of the mean time between (planned!) maintenance (MTBM) and the mean downtime (MDT). *Cf., e.g.,* U.S. DEP'T OF DEF. [DOD], GUIDE FOR ACHIEVING RELIABILITY, AVAILABILITY, AND MAINTAINABILITY § 3.2.4.1 (2005), *available at* http://www.acq.osd.mil/dte/docs/RAM_Guide_080305.pdf; U.K. MINISTRY OF DEFENCE, MOD GUIDE TO R&M TERMINOLOGY USED IN REQUIREMENTS, MINISTRY OF DEFENCE DEFENCE STANDARD 00-49, at 14 (2008), *available at* http://www.dstan.mod.uk/standards/defstans/00/049/00000200.pdf; N. ATL. TREATY ORG. [NATO], NATO R&M TERMINOLOGY APPLICABLE TO ARMPS, ARMP-7, at 2-7, 2-13 (2008), *available at* http://www.nato.int/docu/stanag/armp7/armp-7_ed2-e.pdf.

[19] *Cf.* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 1056 (4th ed. 2008) (noting that "[n]etwork and resource availability often is not fully appreciated until it is gone"). *Cf. also* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 122 (2000).

[20] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 3.4 (2009) (stating that "information systems and networks face security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire and flood"); Paul Hansford, *Physical(Environmental) Security, in* OFFICIAL (ISC)^2 GUIDE TO THE CISSP CBK 281, 283 (Harold F. Tipton ed., 2007) (stating that there

As defined above, information security is primarily only concerned with the security of information. This differs from the definitions of "information security" in U.S. federal law where equal reference is made to the security of both information and information systems.[21] However, by extension, information security as defined here is also concerned with the security of the information systems and networks that store, process, or transmit[22] information because the security of said systems and networks determines the security of the stored, processed, or transmitted information. For example, if a communications network is unavailable, so is the information that could otherwise be communicated over the network.

Information security is, however, not synonymous with "information system security" or "network security" because it also covers information that is not being stored, processed, or transmitted by a system or network, e.g., information printed on paper or stored in any other non-electronic form.

EU institutions generally do not use the term "information security" because it would not allow sufficient differentiation from the domain of national security which is highly sensitive for Member States.[23] Within the EU, the term Network and Information Security (NIS) is

are three basic threat types in the area of physical security: environmental threats, malicious threats, and accidental threats).

[21] *See* Federal Information Security Management Act of 2002 § 301, 44 U.S.C. § 3542(b)(1) (defining "information security" as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity […]; (B) confidentiality […]; and (C) availability […]"); Department of Veterans Affairs Information Security Enhancement Act of 2006 § 902, 38 U.S.C. § 5727(11) (defining "information security" as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability").

[22] From a technical perspective, electronic information can be in either of the following three states: storage, processing, or transmission. *See* JOHN MCCUMBER, ASSESSING AND MANAGING SECURITY RISK IN IT SYSTEMS: A STRUCTURED METHODOLOGY 135 et seq. (2005).

[23] *Cf.* Parliament and Council Regulation 460/2004, art. 1(3), 2004 O.J. (L 77) 1, 4 (EC) (stating that "[t]he objectives and the tasks of the [Network and Information Security Agency] shall be without prejudice to the competencies of the Member States […] which fall outside the scope of the EC Treaty, such as those covered by

used instead. It is defined as “the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.”[24] This definition is narrower than the term “information security” because it does not cover non-electronic information. The same holds true for the term “security of information systems” which was used by the EU before the European Commission introduced the term Network and Information Security in 2001.[25] However, before 2001, the activities in this field were limited to electronic signatures[26] and the recognition of IT security evaluation certificates.[27]

A number of properties other than confidentiality, integrity, and availability are often associated with information security as defined above. These primarily are *authenticity*, *accountability*, *non-repudiation*, *reliability*, and *resilience*.[28] Some of these properties directly

Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security […] and the activities of the State in areas of criminal law”).

[24] Parliament and Council Regulation 460/2004, art. 4(c), 2004 O.J. (L 77) 1, 5 (EC). This definition was first introduced in *Commission Communication on Network and Information Security: Proposal for A European Policy Approach*, at 9, COM (2001) 298 final (June 6, 2001). *See also Commission Communication, A strategy for a Secure Information Society – “Dialogue, partnership and empowerment,”* at 3, COM (2006) 251 final (May 31, 2006) (reiterating the definition provided in COM (2001) 298 final).

[25] *See* Council Decision 92/242, O.J. (L 123) 19 (EEC) (adopting actions “in the field of the security of information systems”: (1) the development of overall strategies for the security of information systems; (2) setting-up the Senior Officials Group Information Systems Security (SOG-IS) with a long-term mandate to advise the Commission on action to be undertaken in the field of the security of information systems).

[26] *See* Parliament and Council Directive 1999/93, O.J. (L 13) 12 (EC) (establishing a legal framework for electronic signatures).

[27] The Commission’s Senior Officials Group Information Systems Security adopted mutual recognition agreements on IT security evaluation certificates in 1997, 1999, and 2010. *See* SENIOR OFFICIALS GROUP INFORMATION SYSTEMS SECURITY, MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES, VERSION 3.0 (2010), *available at* http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/media/formal-docs/mra.pdf.

[28] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.19 (2009) (noting with regard to “information security” that, in addition to confidentiality, integrity, and availability, “other properties,

relate to the security of information while others relate to the security of networks and information systems.

Authenticity (the state of having been successfully authenticated) can be broadly defined as the property that an entity is what it claims to be.[29] More specifically, information authenticity is the property that information originates from or is endorsed by the source which is attributed to that information[30] (e.g. an e-mail was actually sent by the individual identified by the sender address). In this regard, authenticity can be seen as an aspect of information integrity.[31] However, to the extent that authenticity describes the property of users being who they claim to be, it is not so much a property of information security but rather a measure to generally ensure information confidentiality, integrity, and availability.

Accountability can be defined as responsibility of an entity for its actions and decisions.[32] It is therefore not a property of but rather a requirement for certain levels of information security. It should be noted that, practically speaking, maximum accountability requires a full audit

such as authenticity, accountability, non-repudiation, and reliability can also be involved"); *Commission Communication on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"*, COM (2009) 149 final (Mar. 30, 2009) (emphasizing the importance of resilience); SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 280 (4th ed. 2008) (stating that confidentiality, integrity, and availability "branch off into more granular security attributes, such as authenticity, accountability, nonrepudiation, and dependability").

[29] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.6 (2009).

[30] *See* INFORMATION SECURITY MANAGEMENT HANDBOOK 3019 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007). *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.6 (2009) (defining "authenticity" in more abstract terms as the "property that an entity is what it claims to be").

[31] *Cf.* Federal Information Security Management Act of 2002 § 301, 44 U.S.C. § 3542(b)(1)(A) (stating that integrity "includes ensuring information […] authenticity").

[32] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.2 (2009).

trail[33] of all user activities which might be incompatible with a system's confidentiality requirements in terms of anonymity and privacy.

Non-repudiation refers to the ability to prove that the sender has actually sent a given message (non-repudiation of origin) and the receiver has actually received the message (non-repudiation of receipt).[34] This is typically achieved by cryptographic means[35] (i.e. electronic signatures) and can generally be seen as an aspect of information integrity.[36]

Reliability is most often associated with communications networks and information systems.[37] Very generally, it can be defined as the property of consistent intended behavior and results.[38] More specifically, it is "[t]he probability that an item can perform a required function under stated conditions for a given time interval."[39] In practice, it is expressed in terms of Mean

[33] *Cf.* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 34 (3d ed. 2003) (referring to audit as a "type of security").

[34] *See* INFORMATION SECURITY MANAGEMENT HANDBOOK 3102 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007). ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.27 (2009) (defining "non-repudiation" as the "ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event").

[35] *Cf.* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 2 (2d ed. 1996) (stating that cryptography often does not only provide confidentiality, authentication, and integrity but also non-repudiation).

[36] *Cf.* Federal Information Security Management Act of 2002 § 301, 44 U.S.C. § 3542(b)(1)(A) (stating that integrity "includes ensuring information nonrepudiation"); NAT'L COMPUTER SEC. CTR. [NCSC], TRUSTED NETWORK INTERPRETATION, NCSC-TG-005 § 9.1.3 (1987) (also known as the "Red Book"), *available at* http://csrc.nist.gov/publications/secpubs/rainbow/tg005.txt (treating non-repudiation as an aspect of communications integrity).

[37] *See, e.g., Commission Communication, A strategy for a Secure Information Society – "Dialogue, partnership and empowerment,"* at 1, COM (2006) 251 final (May 31, 2006) (noting that "availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society"); *Commission Communication, i2010 – A European Information Society for growth and employment*, at 7, COM (2005) 229 final (June 1, 2005) (stating that information and communications technologies still lack "interoperability, reliability and security").

[38] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.33 (2009).

[39] INT'L TELECOMM. UNION [ITU], QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING – TERMS AND DEFINITIONS RELATED TO THE QUALITY OF

Time Between Failures (MTBF).[40] As noted *supra*, availability is a function of MTBF (and Mean Time To Repair, MTTR). Reliability is therefore an aspect of information security that is fully covered by the concept of information "availability."

Resilience is a term most often used in connection with communications networks—in particular in the context of the Critical Infrastructure Protection (CIP) policy.[41] However, it is a term seldom used in the information security profession.[42] The European Network and Information Security Agency (ENISA)[43] defines it as "the ability of a network to provide and maintain an acceptable level of service in the face of various challenges (unintentional,

TELECOMMUNICATION SERVICES, ITU-T RECOMMENDATION E.800 § 3.1.1.5.5 (2008), *available at* http://www.itu.int/rec/T-REC-E.800-200809-I/en. *See also* IEC, INTERNATIONAL ELECTROTECHNICAL VOCABULARY - CHAPTER 191: DEPENDABILITY AND QUALITY OF SERVICE, IEC 60050-191 (1990) (defining "[r]eliability (as a performance measure)" as "the probability of being able to perform as required under given conditions for the time interval").

[40] *See, e.g.,* Dhananjay Kumar et al., *Availability Modelling of the 3GPP R99 Telecommunication Networks, in* SAFETY & RELIABILITY 977, 978 (Bedford & van Gelder eds., 2003), *available at* http://www.nokia.com/library/files/docs/Availability_Modelling_of_3GPP_R99_Telecommunication_Networks.pdf. *Cf.* ITU, QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING – TERMS AND DEFINITIONS RELATED TO THE QUALITY OF TELECOMMUNICATION SERVICES, ITU-T RECOMMENDATION E.800 § 3.3.16.3 (2008), *available at* http://www.itu.int/rec/T-REC-E.800-200809-I/en (defining "[m]ean time between failures" as "[t]he expectation of the time between failures computed from a statistically significant number of samples usually expressed as the arithmetic mean").

[41] *See Commission Communication on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience",* COM (2009) 149 final (Mar. 30, 2009) (emphasizing the importance of resilience); WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. *Cf. infra* chapter 2.2.2 (discussing the intersections between information security and CIP).

[42] Note that the following sources do not once refer to the concept of resilience: ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 (2009); ISO, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT GUIDELINES FOR TELECOMMUNICATIONS ORGANIZATIONS BASED ON ISO/IEC 27002, ISO/IEC 27011:2008 (2008); INFORMATION SECURITY MANAGEMENT HANDBOOK (Harold F. Tipton & Micki Krause eds., 6th ed. 2007); OFFICIAL (ISC)² GUIDE TO THE CISSP CBK (Harold F. Tipton ed., 2007).

[43] *See* Parliament and Council Regulation 460/2004, 2004 O.J. (L 77) 1 (EC) (establishing ENISA); Parliament and Council Regulation 1007/2008, 2008 O.J. (L 293) 1 (EC) (extending ENISA's mandate until Mar. 14, 2012).

intentional, or naturally caused) affecting their normal operation."[44] This definition is, for all practical purposes, congruent with the concept of availability as described above.[45]

2.2. Related Policy Areas

As a policy area, information security has significant intersections with other important policy areas, in particular with data protection and Critical Infrastructure Protection (CIP).

2.2.1. Data Protection in the EU and Information Privacy in the U.S.

In the EU, the protection of personal data ("data protection") is a very significant policy area, in particular since the adoption of Parliament and Council Directive 95/46[46] (hereinafter *Data Protection Directive* or *EUDPD*) in 1995. Its importance has been elevated in 2009 by the adoption of the Charter of Fundamental Rights of the European Union[47] (hereinafter *Charter*) which declared data protection to be a fundamental right.[48] The EUDPD defines the term "personal data" as "any information relating to an identified or identifiable natural person."[49] This makes clear that—contrary to what the use of the term "data" might imply—"personal

[44] EUROPEAN NETWORK & INFO. SEC. AGENCY [ENISA], GUIDELINES FOR ENHANCING THE RESILIENCE OF COMMUNICATION NETWORKS: PROVIDERS' MEASURES 11 (2009), *available at* http://www.enisa.europa.eu/act/res/providers-measures/files/resilience-good-practices/at_download/fullReport.

[45] *Cf.* EVAN MARCUS & HAL STERN, BLUEPRINTS FOR HIGH AVAILABILITY: DESIGNING RESILIENT DISTRIBUTED SYSTEMS 9 (2000) (defining "resiliency" as "overall system availability").

[46] 1995 O.J. (L 281) 31 (EC).

[47] Charter of Fundamental Rights of the European Union, 2010 O.J. (C 83) 389.

[48] The Charter entered into force with the adoption of the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Dec. 17, 2007, 2007 O.J. (C 306) 1 [hereinafter Lisbon Treaty]. *See* EU Treaty art. 6 (ex EU Treaty art. 6) as amended by the Lisbon Treaty (stating that "[t]he Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties").

[49] EUDPD art. 2(a). The term "identifiable person" is defined as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Id.*

data" is not limited to information that is stored, processed, or transmitted in electronic form.[50]

The EUDPD establishes the following principles: (1) personal data has to be processed fairly and lawfully; (2) it must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (referred to as the principle of "purpose limitation"); (3) personal data has to be adequate, relevant and not excessive in relation to the specified purposes; (4) it must be accurate and, where necessary, kept up to date; and (5) it must be kept in a form which permits identification of data subjects for no longer than is necessary for the specified purposes.[51] Specifically with regard to security, the EUDPD provides that personal data shall be protected "against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access."[52]

The policy area of data protection is therefore wider than the policy area of information security in the sense that it is also concerned with issues other than the confidentiality, integrity, and availability of information. In particular, the central data protection requirement of purpose limitation is not an issue of information security. Furthermore, information security is also generally not concerned with the question to which third parties personal data may be transmitted to.

Data protection is at the same time more narrowly defined than information security. First, it only covers personal data but not any other type of information (e.g. corporate information).

[50] *Cf.* ULRICH DAMMANN & SPIROS SIMITIS, EG-DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE] art. 2 cmt. 4 (1997) (noting the Directive's open wording); Ulrich U. Wuermeling, *Harmonisation of European Union Privacy Law*, 14 J. MARSHALL J. COMPUTER & INFO. L. 411, 432 (1996).

[51] *See* EUDPD art. 6(1)(a)-(e). *Cf. generally* EUGEN EHMANN & MARCUS HELFRICH, EG-DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE] art. 6 cmt. 1 et seq. (1999).

[52] EUDPD art. 17(1).

Second, while the confidentiality and integrity of personal data is fully within the scope of data protection, the availability of personal data is not: the EUDPD only addresses permanent information unavailability ("accidental or unlawful destruction or accidental loss")[53] but does not regard temporary unavailability as an interference with the right to data protection. However, information security clearly covers all types of unavailability of information, may they be permanent or only temporary.

In the U.S., the term data protection is seldom used. To describe a similar policy area, the terms "data privacy" or "information privacy" are often used instead.[54] This policy area is, however, much more fragmented than data protection in the EU and lacks a coherent policy approach.

Under U.S. law, individuals have no comprehensive right to privacy. The common law of torts generally only provides four specific privacy-related torts[55]: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) placing the plaintiff in a false light; and (4) appropriation of the other's name or likeness. While many states, including California, have

[53] EUDPD art. 17(1).

[54] *Cf.* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 56 (2004) (referring to "information privacy law"); Edward J. Eberle, *The Right to Information Self-Determination*, 2001 UTAH L. REV. 965, 983 (referring to "information privacy" when discussing Whalen v. Roe, 429 U.S. 589 (1977)). *Cf. also* Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009). Note that the term "privacy" by itself is too broad as it also includes issues best described as decisional interference. *See* Grinswold v. Connecticut, 381 U.S. 479 (1965) (holding that a Connecticut statute that made the use of contraceptives a criminal offense violated a constitutional right to "privacy"); Roe v. Wade, 410 U.S. 113, 153 (1973) (holding that the right to "privacy" encompasses "a woman's decision whether or not to terminate her pregnancy").

[55] *See* RESTATEMENT (SECOND) OF TORTS § 652A(2) (2009); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960). Compare also Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) which is credited with greatly influencing the judicial acceptance of privacy torts.

adopted these torts, it is notable that New York only recognizes the tort of appropriation of another's name or likeness.[56]

The tort of intrusion upon seclusion requires that the defendant "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of [the plaintiff] or his private affairs or concerns" in a way that "would be highly offensive to a reasonable person."[57] This tort is, however, severely limited because it only applies to the private as opposed to the public sphere.[58] Information regarding one's public life (e.g. one's behavior in public)[59] or information regarding one's private life that has become public is generally outside the scope of this tort.[60]

The tort of public disclosure of private facts requires that the defendant "gives publicity to a matter concerning the private life" of the plaintiff and that the matter publicized is of a kind that "(a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern

[56] *See* Messenger ex rel. Messenger v. Gruner + Jahr Printing and Pub., 727 N.E.2d 549 (N.Y. 2000) (holding that N.Y. does not recognize a common-law right of privacy). *See* N.Y. CIV. RIGHTS LAW §§ 50, 51 (McKinney 2010) (providing a statutory tort against a defendant who "uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person").

[57] RESTATEMENT (SECOND) OF TORTS § 652B (2009). *Cf.* Shulman v. Group W Productions, Inc., 955 P.2d 469, 490 (Cal. 1998) (holding that to prove actionable intrusion, plaintiff must show that (1) the defendant penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff; and (2) the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source).

[58] *Cf.* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 164 (2008) (noting that, "[g]enerally, U.S. courts recognize intrusion-upon-seclusion tort actions only when a person is at home or in a secluded place").

[59] *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (2009) (stating that liability only arises "when [the defendant] has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs"). *Cf.* Sanders v. American Broadcasting Companies, Inc., 978 P.2d 67, 71 (Cal. 1999) (holding that a showing of intrusion as required by the intrusion tort is not made when the plaintiff has merely been observed, or even photographed or recorded in a public place).

[60] *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (2009) (stating that "there is no liability for the examination of a public record concerning the plaintiff, or of documents that the plaintiff is required to keep and make available for public inspection").

to the public."[61] Like the tort of intrusion upon seclusion, this tort only protects the private sphere.[62] Furthermore, "publicity" requires that the plaintiff made the information public "by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[63]

The tort of placing the plaintiff in a false light requires that the defendant "gives publicity to a matter concerning [the plaintiff] that places [him] before the public in a false light" that would "be highly offensive to a reasonable person."[64] Furthermore, it is required that the defendant "had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."[65] Unlike the torts discussed above, this tort is not limited to the private sphere. Its scope is, however, limited by the fact that it requires the same kind of "publicity" as the tort of public disclosure of private facts.[66]

The tort of appropriation of another's name or likeness requires that the defendant "appropriates to his own use or benefit the name or likeness of [the plaintiff]."[67] Liability only attaches if the defendant appropriated the value of the plaintiff's name or likeness such as "the

[61] RESTATEMENT (SECOND) OF TORTS § 652D (2009)

[62] *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (2009) (stating that there is no liability "for giving publicity to facts about the plaintiff's life that are matters of public record" or "for giving further publicity to what the plaintiff himself leaves open to the public eye").

[63] RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (2009).

[64] RESTATEMENT (SECOND) OF TORTS § 652E (2009).

[65] *Id.*

[66] *See id.* cmt. a (referring to § 652D cmt. a).

[67] RESTATEMENT (SECOND) OF TORTS § 652C (2009).

reputation, prestige, social or commercial standing, [or] public interest."[68] Thus, the relevance of this tort in the area of data protection is also limited.

Therefore, common law only protects the confidentiality and integrity of personal information to a very limited extent and does not at all take into account information availability. Statutory state law as well as federal laws implement an industry-specific approach[69] and, to a significant extent, rely on self-regulation.[70] In summary, U.S. law does not provide a comprehensive right to privacy that would at least fully cover information confidentiality and integrity.

[68] RESTATEMENT (SECOND) OF TORTS § 652C cmt. c (2009). *See also id.* (stating that "[u]ntil the value of the name has in some way been appropriated, there is no tort").

[69] Federal privacy laws include the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) which covers health plans, health care clearinghouses, health care providers, and their business associates, the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) which covers financial institutions, the Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114 (1970) which covers credit reporting agencies (CRAs), entities that furnish information to CRAs, and those who use credit reports, the Drivers Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 (1994) which covers state departments of motor vehicles, the Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988) which covers video tape service providers, and the Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) which covers federal agencies. For a more extensive list see DANIEL J. SOLOVE, INFORMATION PRIVACY LAW 36 (2008); *Cf. also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 67 (2004) (stating that "Congress has passed a series of statutes narrowly tailored to specific privacy problems"). Examples for state laws include the California Financial Information Privacy Act, 2003 Cal. Legis. Serv. Ch. 241 (West) (codified at CAL. FIN. CODE §§ 4050-60) which covers financial institutions, and the California Confidentiality of Medical Information Act, 1981 Cal. Legis. Serv. Ch. 782 (West) (codified at CAL. CIV. CODE § 56 et seq.) which covers medical providers, health plans, pharmaceutical companies, and many businesses organized for the purpose of maintaining medical information.

[70] *Cf.* Lauren B. Movius & Nathalie Krup, *U.S. and EU Privacy Policy: Comparison of Regulatory Approaches*, 3 INT'L J. OF COMM. 169, 174 (2009) (stating that the history of privacy regulations in the U.S. has been one of industry self-regulation and reactive legislation); U.S. DEP'T OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997), *available at* http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm. *Cf. also* CHRIS JAY HOOFNAGLE, PRIVACY SELF REGULATION: A DECADE OF DISAPPOINTMENT (2005), *available at* http://epic.org/reports/decadedisappoint.pdf (arguing extensively that the experience with privacy self-regulation online points to a sustained failure of business to provide reasonable privacy protections); ROLAND VOGL, THE EU-U.S PRIVACY CONTROVERSY: A QUESTION OF LAW OR GOVERNANCE? 22 (2000), *available at* http://sls-stage.stanford.edu/publications/dissertations_theses/diss/VoglRoland-tft2000.pdf (arguing that the reason why the EU's approach is regulatory while the U.S.'s is largely self-regulatory is that the EU follows a fundamental right approach while the U.S. follows a market oriented approach).

This raises the question whether the security of personal information is a legitimate policy field in the U.S. Why should we be concerned with protecting the confidentiality, integrity, and availability of personal information from malicious threat agents or accidents when the law does not generally prohibit entities that legitimately process personal information from disclosing, altering, or destroying personal information as they wish? The answer to this question is that a privacy regime that largely relies on self-regulation necessarily does not give comprehensive legal rights to the individuals concerned. However, individuals nevertheless have a legitimate interest in their privacy[71] and, by extension, the security of their personal information, irrespective of whether the privacy is protected by government regulation or only self-regulation.[72]

This thesis often refers to concepts related to EU data protection law and U.S. data privacy law. To emphasize that personal data (as defined by the EUDPD) is a specific type of information—that may or may not be electronic—and to avoid any association with the EUDPD where none is intended, this thesis will use the more neutral term *personal*

[71] It is often suggested that people only claim to care about privacy but demonstrate by their actions that they actually do not. However, such a conclusion is not permissible if the social context in which people are willing to share their personal information is not considered. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 150, 186 et seq. (2010). Furthermore, some of the actions often claimed to invalidate stated privacy preferences are indeed entirely rational, even if one values privacy. *See*, PAUL SYVERSON, THE PARADOXICAL VALUE OF PRIVACY (SECOND WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, WORKING PAPER, 2003), *available at* http://www.cpppe.umd.edu/rhsmith3/papers/Final_session3_syverson.pdf (arguing that disclosing personal information for a free hamburger may not be inherently irrational with respect to claimed valuation of privacy since the expectation of how the information will be used dominates a cost-benefit analysis); Adam Shostack & Paul Syverson, *What Price Privacy (and why identity theft is about neither identity nor theft), in* ECONOMICS OF INFORMATION SECURITY 129, 132 (L. Jean Camp & Stephen Lewis eds., 2004).

[72] For example, a recent study showed, with regard to young adults, a relatively strong discrepancy between the perceived and the actual privacy protections provided by the law. *See* CHRIS HOOFNAGLE ET AL., HOW DIFFERENT ARE YOUNG ADULTS FROM OLDER ADULTS WHEN IT COMES TO INFORMATION PRIVACY ATTITUDES AND POLICIES? 20 (2010), http://ssrn.com/abstract=1589864 (stating that 18-24 year olds are more likely to believe that the law protects their privacy online and offline more than it actually does). *Cf.* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 185 (2008) (stating that divergences between the ways different societies protect privacy do not necessarily stem from conceptual differences about privacy).

information to refer to the concept of "personal data" as defined in the EUDPD. The term "personal data" will only be used in the context of EU data protection law.

Similarly, to refer to entities that "[determine] the purposes and means of the processing of personal data" (referred to as "data controllers" in the EUDPD),[73] this thesis will use the term *personal information controllers*. Entities "which [process] personal data on behalf of the controller" (referred to as "processors" in the EUDPD)[74] will be referred to as *personal information processors*.

For example, if a retailer collects personal information from its customers and outsources its data processing operations to a second company, the retailer would be then referred to as the personal information controller while the second company would be referred to as a personal information processor.

This terminology intends to be more intuitive by making clear what type of information is being controlled or processed while not presupposing any specific privacy regime.

2.2.2. Critical Infrastructure Protection

The policy area of Critical Infrastructure Protection (CIP) generally deals with the protection of assets which are essential for the maintenance of vital societal functions. In the U.S. this policy area was first addressed in 1998 by Presidential Decision Directive/PDD-63[75] which

[73] EUDPD art. 2(d).

[74] EUDPD art. 2(e).

[75] *See* The White Paper on Critical Infrastructure Protection PDD 63, 1998 WL 263839, at *1 (May 22, 1998) (stating that "[c]ritical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government").

was superseded by Homeland Security Presidential Directive/HSPD-7[76] in 2003. The USA PATRIOT Act[77] also addresses the issue and defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[78]

In the EU, the main legislative act is Council Directive 2008/114[79] (hereinafter *CIP Directive*) which is only concerned with "European critical infrastructure" (ECI) which is defined as "critical infrastructure"[80] the disruption of which "would have a significant impact on at least two Member States."[81] Furthermore, the CIP Directive is currently limited to two sectors: energy and transport.[82]

As a policy area, CIP concerns a wide range of industry sectors such as transportation, energy, water, and information and communication technology (ICT). It is this last sector which is

[76] Homeland Security Presidential Directive/HSPD–7—Critical Infrastructure Identification, Prioritization, and Protection, 2 PUB. PAPERS 1739 (Dec. 17, 2003).

[77] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001).

[78] USA PATRIOT Act § 1016, 42 U.S.C. § 5195c(e).

[79] Council Directive 2008/114, 2008 O.J. (L 345) 75 (EC).

[80] *See* CIP Directive art. 2(a) (defining "critical infrastructure" as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"). Note that this definition is based on the concept of territoriality. This would raise problems if the CIP Directive were amended to also cover the ICT sector because satellites clearly defy the concept of territoriality.

[81] *See* CIP Directive art. 2(b).

[82] *See* CIP Directive art. 3(3). Note, however, that the CIP Directive acknowledges "the need to include other sectors within its scope, inter alia, the information and communication technology ('ICT') sector." CIP Directive recital 5.

most relevant with regard to information security and has evolved into a distinguishable policy area: Critical Information Infrastructure Protection (CIIP).[83]

CIIP is primarily concerned with ensuring the availability of the information infrastructure. Since availability of that infrastructure is a pre-condition for the availability of many information assets, CIIP can be considered a sub-set of the policy area of information security. Since information security is not only concerned with the availability but also with the confidentiality and integrity of information, it is much broader than the policy area of CIIP. Furthermore, CIIP is also limited to "critical" assets, while information security generally covers all information assets.

In the EU, CIIP is dominated by non-regulatory policy initiatives such as facilitating information sharing between Member States or fostering the cooperation between the public and the private sector by establishing a public private partnership.[84] Similarly, the U.S. has also attempted to address CIIP issues by creating public private partnerships and private-sector Information Sharing and Analysis Centers (ISACs).[85] However, due to their non-regulatory nature, such initiatives are outside the scope of this thesis.

[83] *Cf. Commission Communication on Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"*, COM (2009) 149 final (Mar. 30, 2009). *Cf. also* MYRIAM DUNN & ISABELLE WIGERT, INTERNATIONAL CIIP HANDBOOK 2004—AN INVENTORY AND ANALYSIS OF PROTECTION POLICIES IN FOURTEEN COUNTRIES (2004), *available at* http://kms1.isn.ethz.ch/serviceengine/Files/ISN/452/ipublicationdocument_singledocument/72b87f2b-61bd-4122-acbf-4c689532036a/en/doc_454_290_en.pdf; NAT'L ACAD. OF ENG'G, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES (Stewart D. Personick & Cynthia A. Patterson eds., 2003).

[84] *Commission Communication on Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"*, at 8, COM (2009) 149 final (Mar. 30, 2009).

[85] *See* MYRIAM DUNN & ISABELLE WIGERT, INTERNATIONAL CIIP HANDBOOK 2004—AN INVENTORY AND ANALYSIS OF PROTECTION POLICIES IN FOURTEEN COUNTRIES 212 et seq. (2004), *available at* http://kms1.isn.ethz.ch/serviceengine/Files/ISN/452/ipublicationdocument_singledocument/72b87f2b-61bd-4122-acbf-4c689532036a/en/doc_454_290_en.pdf. To protect any information that is revealed by the private

Lastly, it should be noted that CIP sectors other than ICT also have intersections with information security to the extent that they rely on the confidentiality, integrity, or availability of information. As will be further discussed *infra* in chapter 4.3.2, one prominent example is the energy sector which heavily uses computer systems to monitor and control the bulk-power system (referred to as *Supervisory Control and Data Acquisition* or *SCADA* systems). Recent attacks on SCADA systems by a malware known as "Stuxnet" have highlighted the importance of information security in this field.[86]

2.3. Actors in the Information Security Landscape

To facilitate the analysis of regulatory policies in the field of information security, a discussion of the most significant types of actors in this field is warranted. Given that information security generally presents itself as the same problem for every sector of industry (e.g. financial institutions or healthcare providers), the following categorization will not be sector-specific but will rather focus on the roles different actors play from a technological, risk-based perspective.

sector to the U.S. government, from mandatory disclosure pursuant to the Freedom of Information Act, the Critical Infrastructure Information Act of 2002 was passed as title II, subtitle B of the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002). *Cf.* NAT'L ACAD. OF ENG'G, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES 25 et seq. (Stewart D. Personick & Cynthia A. Patterson eds., 2003) (discussing why the Freedom of Information Act had been perceived as a barrier to the sharing of critical infrastructure information).

[86] Stuxnet is a specialized malware targeting SCADA systems running Siemens SIMATIC WinCC or SIMATIC Siemens STEP 7 software. It propagates via USB-drives or open network shares by exploiting the vulnerabilities CVE-2010-2568, CVE-2010-2729, and CVE-2008-4250 in the Windows operating system. *See* NICOLAS FALLIERE ET AL., SYMANTEC CORP., W32.STUXNET DOSSIER (2010), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Note that there are also reasons to believe that the Northeast Blackout of 2003 affecting about 55 million people may have been caused by a malware known as *Blaster*. *See* Bruce Schneier, *Blaster and the great blackout*, SALON.COM, Dec. 16, 2003, http://dir.salon.com/story/tech/feature/2003/12/16/blaster_security/index.html.

2.3.1. Providers of Communications Services

The term *communications service provider* is used here to describe Internet access providers, Internet backbone providers, and providers that operate the public switched telephone network (PSTN). Given its importance, the architecture of the Internet infrastructure will be discussed in some detail below.

From an architectural perspective, the Internet can be described as a packet-based[87] global network of interconnected autonomous networks (referred to as *Autonomous Systems* or *ASes*)[88] that is based on the TCP/IP protocol suite.[89] Each AS is assigned one or more Internet Protocol (IP) address ranges[90] and a unique Autonomous System Number (ASN).[91] To route

[87] On a packet-based network (as opposed to a circuit-switched network like the PSTN), data has to be broken down into suitably-sized blocks called packets in order to be transferred over the network.

[88] *See* J. HAWKINSON & T. BATES, GUIDELINES FOR CREATION, SELECTION, AND REGISTRATION OF AN AUTONOMOUS SYSTEM (AS), RFC 1930, at 2 (1996), ftp://ftp.rfc-editor.org/in-notes/rfc1930.txt (defining "AS" as "a connected group of one or more IP prefixes run by one or more network operators which has a *single* and *clearly defined* routing policy").

[89] The TCP/IP protocol suit consists of various protocols implemented on (1) the link layer: e.g. Ethernet, Digital Subscriber Line (DSL), or Fiber Distributed Data Interface (FDDI); (2) the network layer: e.g. the Internet Protocol (IP); (3) the transport layer: e.g. the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP); and (4) the application layer: e.g. the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP). *See* W. RICHARD STEVENS, TCP/IP ILLUSTRATED, VOLUME 1: THE PROTOCOLS 2 (1994). *Cf. also* 47 U.S.C. § 230(f)(1) (defining "Internet" as "the international computer network of both Federal and non-Federal interoperable packet switched data networks").

[90] In general, a (public) IP address uniquely identifies a computer's network interface on the Internet. Under Internet Protocol version 4 (IPv4), IP addresses are 32-bit numbers (i.e. 0 to 4,294,967,295) where each octet (8 bits) is usually written as a decimal number (0-255), e.g. 171.67.216.14. Under Internet Protocol version 6 (IPv6) 128-bit numbers (i.e. 0 to 2^{128}) are used instead. An IP address range (often referred to as a routing prefix) is typically expressed in the Classless Inter-Domain Routing (CIDR) notation as an IP address in combination with the number of bits that are constant for all IP addresses within the range, e.g., 171.67.216.0/24 for 171.67.216.0 to 171.67.216.255. *Cf.* V. FULLER & T. LI, CLASSLESS INTER-DOMAIN ROUTING (CIDR): THE INTERNET ADDRESS ASSIGNMENT AND AGGREGATION PLAN, RFC 4632, at 4 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4632.txt.

[91] *Cf.* J. HAWKINSON & T. BATES, GUIDELINES FOR CREATION, SELECTION, AND REGISTRATION OF AN AUTONOMOUS SYSTEM (AS), RFC 1930, at 3 (1996), ftp://ftp.rfc-editor.org/in-notes/rfc1930.txt.

IP packets within an AS, an interior gateway protocol (IGP)[92] is used while an exterior gateway protocol,[93] typically the Border Gateway Protocol (BGP),[94] is used to route packets to other ASes. The computers that actually perform routing operations are referred to as *routers*.[95]

Since there are over 34,000 ASes worldwide,[96] no AS has a direct connection to all other ASes. Most ASes only have a single connection to their upstream AS which in turn might have multiple connections to other larger ASes. This means that an IP packet might travel through multiple ASes until it reaches its destination. To achieve a certain level of redundancy, lager ASes typically also have multiple routes over different ASes to a single destination AS.

In order to know which ASes have a route or, often equally important, the best route to a particular IP address range, each AS uses BGP to build a global routing table that lists routs for each IP address range assigned to an AS.[97] This routing table is built in an automatic and decentralized fashion: Each AS announces to its peers the IP address ranges that were

[92] Commonly used IGPs are the Routing Information Protocol (RIP), the Interior Gateway Routing Protocol (IGRP), the Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF). *See* RAVI MALHOTRA, IP ROUTING 10, 33, 63, 107 (2002) (describing each of the aforementioned IGPs).

[93] Note that the term "Exterior Gateway Protocol" is used here exclusively to refer to inter-AS routing protocols in general and not to the specific inter-AS routing protocol specified in D.L. MILLS, EXTERIOR GATEWAY PROTOCOL FORMAL SPECIFICATION, RFC 904 (1984), ftp://ftp.rfc-editor.org/in-notes/rfc904.txt.

[94] Border Gateway Protocol 4 (BGP-4) has become the de-facto standard as an exterior gateway protocol. It is specified in Y. REKHTER ET AL., A BORDER GATEWAY PROTOCOL 4 (BGP-4), RFC 4271 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4271.txt. *Cf.* RAVI MALHOTRA, IP ROUTING 157 (2002).

[95] Each AS typically contains a large number of routers. *Cf.* RAVI MALHOTRA, IP ROUTING 6 (2002).

[96] As of Feb. 10, 2011, there are 35,825 ASes. *See* http://thyme.apnic.net/ap-data/2011/02/10/0400/mail-global (last accessed Feb. 10, 2011).

[97] BGP-4 allows for route aggregation which actually reduces the number of IP address ranges that have to be stored in a global routing table. *See* Y. REKHTER ET AL., A BORDER GATEWAY PROTOCOL 4 (BGP-4), RFC 4271, at 86 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4271.txt.

assigned to it as well as the IP address ranges for which it knows a route (via another AS).[98] ASes that only announce their own IP address ranges are known as "stub ASes"[99] while those that announce their willingness to also transport traffic to another AS are called a "transit AS."[100]

This leaves one important question: Who may operate an AS? AS numbers (ASNs) and IP address ranges are initially assigned by the Internet Assigned Numbers Authority (IANA)[101] to Regional Internet Registries (RIRs)[102] which in turn finally assign them to Local Internet Registries (LIRs).[103] These commonly are Internet backbone providers, Internet access providers, or large corporations that require a large IP address space. Consumers and all but very few corporations turn to Internet access providers to obtain public IP addresses. By doing so, they effectively become part of their Internet access provider's AS.

In light of the above discussion, Internet backbone providers are defined here as entities that operate a transit AS. Internet access providers are defined as all other entities that provide

[98] *Cf.* RAVI MALHOTRA, IP ROUTING 166 et seq. (2002).

[99] As of Feb. 10, 2011, 30,874 or 86.2% of all ASes are stubs. *See* http://thyme.apnic.net/ap-data/2011/02/10/0400/mail-global (referring to stub ASes as "origin-only ASes"; last accessed Feb. 10, 2011). *Cf. also* Y. REKHTER & P. GROSS, APPLICATION OF THE BORDER GATEWAY PROTOCOL IN THE INTERNET, RFC 1772, at 3 (1995), ftp://ftp.rfc-editor.org/in-notes/rfc1772.txt (defining "stub AS" as "an AS that has only a single connection to one other AS" and therefore "only carries local traffic").

[100] *Cf. id.* (defining "transit AS" as "an AS that has connections to more than one other AS, and is designed (under certain policy restrictions) to carry both transit and local traffic"). As of Feb. 10, 2011, 4951 or 13.8% of all ASes are transit ASes which also announce their own IP address ranges; 122 or 0.3% are transit-only ASes. *See* http://thyme.apnic.net/ap-data/2011/02/10/0400/mail-global (last accessed Feb. 10, 2011).

[101] IANA is operated by the Internet Corporation for Assigned Names and Numbers (ICANN). *Cf. infra* note 146.

[102] There are five RIRs: African Network Information Centre (AfriNIC), American Registry for Internet Numbers (ARIN), Asia-Pacific Network Information Centre (APNIC), Latin American and Caribbean Internet Addresses Registry (LACNIC), and Réseaux IP Européens Network Coordination Centre (RIPE NCC). For the ASNs currently assigned by IANA to RIRs see http://www.iana.org/assignments/as-numbers/as-numbers.xml (last accessed Feb. 10, 2011).

[103] Membership in an RIR is typically required to become an LIR. *Cf.* http://www.ripe.net/lir-services/member-support (last accessed Feb. 10, 2011)

Internet access to third parties.[104] Users typically have a contractual relationship with their Internet access provider but not with any of the Internet backbone providers. The connection between different providers (ASes) might be established on a contractual or on a voluntary basis.

It is important to note that the core communication infrastructure of the Internet does not only consist of the IP routing services described above. There is also another type of service on which practically all online services depend: the Domain Name System (DNS). However, since DNS is not a communications service it will be discussed in the context of other online services in the following chapter.

The availability of the Internet's core infrastructure is a *conditio sine qua non* for the availability of most electronically stored information. Furthermore, vulnerabilities in this infrastructure may also threaten the confidentiality and integrity of information that is transferred over communications networks.[105]

Lastly, it should be pointed out that the electrical power industry, while not directly playing a significant role in the information security landscape, provides the power on which all communications networks and information systems depend. Accordingly, information security threats that may affect the operations of the electrical grid are of greatest concern for the availability of all electronic information.

[104] Note that an Internet access provider may also function as an Internet backbone provider if it operates a transit AS rather than a stub AS.

[105] For example, by manipulating DNS information, a malicious threat agent may be able to redirect traffic destined for a certain server to his own computer, thereby enabling him to compromise the confidentiality and integrity of the transferred data. This is referred to as a "man in the middle" attack. *See* IAN GREEN, DNS SPOOFING BY THE MAN IN THE MIDDLE 16 (2005), *available at* http://www.sans.org/reading_room/whitepapers/dns/dns-spoofing-man-middle_1567 (discussing how a certain vulnerability in the Windows XP DNS resolver could be used to perform a man in the middle attack).

2.3.2. Providers of Online Services

In general terms, online services can be defined as services that are offered *over* the Internet—as opposed to services that offer access *to* the Internet. To provide a more technical differentiation from Internet access and Internet backbone providers, the networking model of the TCP/IP protocol suite serves as a helpful tool. The TCP/IP networking model consists of four layers: (1) the link layer, (2) the network layer, (3) the transport layer, and (4) the application layer.[106]

The *link layer* (often also referred to as data link layer) handles the hardware details of physically interfacing with the network.[107] Depending on the type of medium the network uses, different protocols are employed on this layer, e.g., Ethernet,[108] Digital Subscriber Line (DSL),[109] or Fiber Distributed Data Interface (FDDI).[110]

[106] *Cf.* R. BRADEN, REQUIREMENTS FOR INTERNET HOSTS — COMMUNICATION LAYERS, RFC 1122 (1989), ftp://ftp.rfc-editor.org/in-notes/rfc1122.txt. Note that the TCP/IP networking model is distinct from the Open Systems Interconnection (OSI) Model which is composed of seven layers. *Cf.* ISO & IEC, INFORMATION TECHNOLOGY — OPEN SYSTEMS INTERCONNECTION — BASIC REFERENCE MODEL: THE BASIC MODEL, ISO/IEC 7498-1:1994 (1994).

[107] *Cf.* W. RICHARD STEVENS, TCP/IP ILLUSTRATED, VOLUME 1: THE PROTOCOLS 2 (1994). Note that the link layer in the TCP/IP model corresponds to the physical layer and the data link layer in the OSI model. *See* ISO & IEC, INFORMATION TECHNOLOGY — OPEN SYSTEMS INTERCONNECTION — BASIC REFERENCE MODEL: THE BASIC MODEL, ISO/IEC 7498-1:1994 §§ 7.6, 7.7 (1994).

[108] Ethernet is typically used in a local area network (LAN); it is specified in INST. OF ELECTRICAL AND ELECTRONICS ENGINEERS [IEEE], IEEE STANDARD FOR INFORMATION TECHNOLOGY—TELECOMMUNICATIONS AND INFORMATION EXCHANGE BETWEEN SYSTEMS—LOCAL AND METROPOLITAN AREA NETWORKS—SPECIFIC REQUIREMENTS—PART 3: CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION (CSMA/CD) ACCESS METHOD AND PHYSICAL LAYER SPECIFICATIONS, IEEE 802.3-2008 (2008), *available at* http://standards.ieee.org/getieee802/802.3.html.

[109] DSL is used over the wires of a local telephone network. There are many DSL variants that generally can be classified as Symmetric DSL (SDSL) where the upstream and downstream bandwidth are the same and Asymmetric DSL (ADSL) where typically the downstream bandwidth is much higher than the upstream bandwidth. *Cf.* Edward Jones, *Introduction to DSL, in* FUNDAMENTALS OF DSL TECHNOLOGY 119, 125 (Philip Golden et al. eds., 2006).

[110] Since FDDI is based on optical data transmission, it can operate over long distances. It is therefore typically used as a backbone for larger networks. FDDI standards include ISO, INFORMATION PROCESSING SYSTEMS — FIBRE DISTRIBUTED DATA INTERFACE (FDDI) — PART 1: TOKEN RING PHYSICAL LAYER PROTOCOL (PHY), ISO

The *network layer* (sometimes referred to as the Internet layer) is responsible for the movement of packets from their source to their destination. This function is performed by the Internet Protocol (IP)[111] and is referred to as IP routing. Currently, IP version 4 (IPv4)[112] is most widely used on the Internet. However, since IANA has assigned the last available IP address ranges to Regional Internet Registries on January 31, 2011,[113] the use of IPv6[114] is expected to increase significantly in the future.

The *transport layer* controls the flow of data between two networked computers (also referred to as *hosts*). The TCP/IP protocol suite provides two very different protocols for this purpose: the Transmission Control Protocol (TCP)[115] and the User Datagram Protocol (UDP).[116] TCP is connection-oriented in the sense that it requires that a connection is explicitly established before any data is exchanged.[117] It also provides reliability by mandating that an

9314-1:1989 (1989); ISO, INFORMATION PROCESSING SYSTEMS — FIBRE DISTRIBUTED DATA INTERFACE (FDDI) — PART 2: TOKEN RING MEDIA ACCESS CONTROL (MAC), ISO 9314-2:1989 (1989), and ISO & IEC, INFORMATION PROCESSING SYSTEMS — FIBRE DISTRIBUTED DATA INTERFACE (FDDI) — PART 3: PHYSICAL LAYER MEDIUM DEPENDENT (PMD), ISO/IEC 9314-3:1990 (1990).

[111] Other protocols present on the network layer include the Internet Control Message Protocol (ICMP) which provides diagnostic and error functionality for IP and the Internet Group Management Protocol (IGMP) which is used to manage simultaneous one-to-many communications (multicasting). *Cf.* J. POSTEL, INTERNET CONTROL MESSAGE PROTOCOL, RFC 792 (1981), ftp://ftp.rfc-editor.org/in-notes/rfc792.txt; B. CAIN ET AL., INTERNET GROUP MANAGEMENT PROTOCOL, VERSION 3, RFC 3376 (2002), ftp://ftp.rfc-editor.org/in-notes/rfc3376.txt.

[112] *See* J. POSTEL, INTERNET PROTOCOL—DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 791 (1981), ftp://ftp.rfc-editor.org/in-notes/rfc791.txt.

[113] *See* Number Resource Org. [NRO], Free Pool of IPv4 Address Space Depleted (Feb. 3, 2011), http://www.nro.net/news/ipv4-free-pool-depleted. *Cf.* Johannes Ullrich, *FAQ To IPv4 Exhaustion*, SANS INTERNET STORM CENTER, Feb. 1, 2011, http://isc.sans.edu/diary.html?storyid=10342.

[114] *See* S. DEERING & R. HINDEN, INTERNET PROTOCOL, VERSION 6 (IPV6) SPECIFICATION, RFC 2460 (1998), ftp://ftp.rfc-editor.org/in-notes/rfc2460.txt.

[115] *See* J. POSTEL, TRANSMISSION CONTROL PROTOCOL, RFC 793 (1981), ftp://ftp.rfc-editor.org/in-notes/rfc793.txt.

[116] *See* J. POSTEL, USER DATAGRAM PROTOCOL, RFC 768 (1980), ftp://ftp.rfc-editor.org/in-notes/rfc768.txt.

[117] This is done by performing a “three way handshake.” *See* J. POSTEL, TRANSMISSION CONTROL PROTOCOL, RFC 793, at 26 (1981), ftp://ftp.rfc-editor.org/in-notes/rfc793.txt.

acknowledgement packet is sent for each packet that has been received.[118] This way, TCP can provide a stream of bytes to application layer protocols that therefore do not have to concern themselves with the handling of individual packets. UDP, on the other hand, is not connection-oriented, does not implement reliability measures, and requires application layer protocols to handle individual packets.[119]

The *application layer* handles the details of the particular application. For example, for browsing the world wide web, the Hypertext Transfer Protocol (HTTP)[120] is used while the Simple Mail Transfer Protocol (SMTP)[121] is used to transfer e-mails between mail servers.

When a web browser which implements the application layer protocol HTTP wants to transfer data to a web server, it passes that data down the operating system's protocol stack where it travels through the remaining three layers where each adds certain information in a process that is referred to as encapsulation: On the transport layer, TCP will break up the data into individual packets (referred to as TCP segments) and will prepend a header to the data that contains TCP-specific information such as a source port number and a destination port number.[122] On the network layer, the Internet Protocol will prepend a header that contains IP-specific information such as the source IP address and the destination IP address. On the link

[118] *See id.* at 9.

[119] *Cf.* W. RICHARD STEVENS, TCP/IP ILLUSTRATED, VOLUME 1: THE PROTOCOLS 143 (1994).

[120] *See* R. FIELDING ET AL., HYPERTEXT TRANSFER PROTOCOL — HTTP/1.1, RFC 2616 (1999), ftp://ftp.rfc-editor.org/in-notes/rfc2616.txt.

[121] J. KLENSIN, SIMPLE MAIL TRANSFER PROTOCOL, RFC 5321 (2008), ftp://ftp.rfc-editor.org/in-notes/rfc5321.txt.

[122] TCP and UDP use so-called port numbers (0 to 65535) to identify particular applications. In order for a client (e.g. a web browser) to know which server port to connect to, IANA provides a list of *well-known* ports (0 to 1023) and a list of *registered* ports. For example, HTTP has been assigned port 80. *See* http://www.iana.org/assignments/port-numbers (last accessed Feb. 10, 2011). *Cf. also* W. RICHARD STEVENS, TCP/IP ILLUSTRATED, VOLUME 1: THE PROTOCOLS 12 (1994).

layer, a protocol such as Ethernet will prepend a header containing certain link layer protocol specific information (e.g. the source and the destination hardware address of the communicating network interfaces).[123] When such a packet travels through the Internet, from one AS to another and, within an AS, from one router to another, each router will need to examine only the first two headers which correspond to the link layer and the network layer: the link layer will take care of the hardware-related aspects of the packet transmission while the network layer (i.e. the Internet Protocol) will allow the router to determine where to route the packet by examining the packet's destination IP address. On the other hand, the transport layer and the application layer are of no interest to an Internet access provider or Internet backbone provider when performing standard-based IP routing.[124] Transport and application layer protocols are typically only implemented by the end nodes of the network. Much of the intelligence of the Internet is therefore not provided by its core infrastructure but rather by the end nodes of the network.[125] Those end nodes can generally be classified as servers or clients.

[123] When Ethernet is used at the link layer, this address is referred to as the Media Access Control (MAC) address. *See* IEEE, IEEE STANDARD FOR INFORMATION TECHNOLOGY—TELECOMMUNICATIONS AND INFORMATION EXCHANGE BETWEEN SYSTEMS—LOCAL AND METROPOLITAN AREA NETWORKS—SPECIFIC REQUIREMENTS—PART 3: CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION (CSMA/CD) ACCESS METHOD AND PHYSICAL LAYER SPECIFICATIONS, IEEE 802.3-2008 §§ 3.2.4-5 (2008), *available at* http://standards.ieee.org/getieee802/802.3.html. *Cf. also* CHARLES E. SPURGEON, ETHERNET: THE DEFINITIVE GUIDE 25 (2000).

[124] Note that some providers do advocate the analysis of transport and application layer data in order to perform traffic prioritization based on the type of traffic involved. Such efforts are, however, contrary to the basic architecture of the Internet. *See* BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION 107 (2010).

[125] This is often also referred to as the "end-to-end principle." *Cf.* R. BUSH & D. MEYER, SOME INTERNET ARCHITECTURAL GUIDELINES AND PHILOSOPHY, RFC 3439, at 2 (2002), ftp://ftp.rfc-editor.org/in-notes/rfc3439.txt; Jerry H. Saltzer et al., *End-To-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYS. 277 (1984); Marjory S. Blumenthal & David D. Clark, *Rethinking the Design of the Internet: the End-to-End Arguments vs. the Brave New World*, 1 ACM TRANSACTIONS ON INTERNET TECH. 70 (2001). It is this property of the Internet that enables what *Zittrain* calls "generativity," fosters what *Benkler* refers to as the non-market based production of information in the networked information economy and, as *Lessig* argues, fosters commercial and cultural innovation. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 70 (2008); YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 146 (2006); LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 35 (2001). It is also this issue that is at the heart of the net neutrality

Servers are those computers that offer services over the Internet while clients are those computers that use said services.[126]

In light of the above discussion, providers of online services can therefore be defined, from a technical perspective, as providers that operate servers that offer services on the transport layer and the application layer.

In a first step, online services can be classified by the type of application layer protocol they use. For example, e-mail services use the Simple Mail Transfer Protocol (SMTP)[127] while Voice over IP (VoIP) services usually use the Real-time Transport Protocol (RTP),[128] H.323,[129] or a proprietary protocol.[130] Finally, services offered via a website use HTTP.[131]

However, classifications by the application layer protocol used have become somewhat obsolete because many services that previously used their own protocol have been

debate. *Cf., e.g.,* Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 95 GEO. L.J. 1847 (2006); Brett M. Frischmann & Barbara van Schewick, *Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo,* 47 JURIMETRICS 383 (2007).

[126] *Cf.* W. RICHARD STEVENS, TCP/IP ILLUSTRATED, VOLUME 1: THE PROTOCOLS 12 (1994). Note that peer-to-peer (P2P) services like file sharing networks do not use the traditional client-server model.

[127] Additionally, the Internet Message Access Protocol (IMAP) and the Post Office Protocol version 3 (POP3) are often used to allow users to read their mails.

[128] Typically used in conjunction with the Session Initiation Protocol (SIP). *Cf.* H. SCHULZRINNE ET AL., RTP: A TRANSPORT PROTOCOL FOR REAL-TIME APPLICATIONS, RFC 3550 (2003), ftp://ftp.rfc-editor.org/in-notes/rfc3550.txt; J. ROSENBERG ET AL., SIP: SESSION INITIATION PROTOCOL, RFC 3261 (2002), ftp://ftp.rfc-editor.org/in-notes/rfc3261.txt.

[129] *See* ITU, PACKET-BASED MULTIMEDIA COMMUNICATIONS SYSTEMS, ITU-T RECOMMENDATION H.323 (2009), *available at* http://www.itu.int/rec/T-REC-H.323-200912-P/en.

[130] Most famously, Skype uses a proprietary protocol. *Cf.* Salman A. Baset & Henning Schulzrinne, *An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol,* 25 IEEE INT'L CONF. ON COMPUTER COMM. 2695 (2006).

[131] The services on the Internet that use HTTP are collectively referred to as the World Wide Web.

reengineered to use HTTP in order to integrate them into websites. Examples include reading and sending mails,[132] Usenet discussions,[133] instant messaging,[134] and file transfers.[135]

Furthermore, it is important to recognize that more and more desktop applications are being migrated to the web. A desktop application is a software that, in order to be used, has to be installed on each user's computer. Once migrated to the web, these applications run on the provider's servers and not the users' computers. All that is left for a user's computer to do is to visualize a user interface (typically via a web browser) with which users can interact. The concept of migrating applications from the users' computers to the provider's servers was introduced in the 1990s as Application Service Providing (ASP) but only recently gained significant traction, now being loosely referred to as "cloud computing."[136]

[132] With the emergence of services like Gmail, Yahoo! Mail, and Windows Live Hotmail, the Internet Message Access Protocol (IMAP), the Post Office Protocol version 3 (POP3), and SMTP (as regards mail submission from a client to a mail server) have been widely displaced by webmail services.

[133] Usenet has been practically replaced by web-based bulletin board systems (e.g. phpBB).

[134] Applications like ICQ, AOL Instant Messenger (AIM), or MSN Messenger (now Windows Live Messenger) have largely been replaced by Facebook, a web-based social networking platform.

[135] The File Transfer Protocol (FTP) used to be the primary means of transferring files. *Cf.* J. POSTEL & J. REYNOLDS, FILE TRANSFER PROTOCOL (FTP), RFC 959 (1985), ftp://ftp.rfc-editor.org/in-notes/rfc959.txt. Today, most file transfers a performed via HTTP-based file uploads.

[136] *Cf.* NAT'L INST. OF STANDARDS & TECH. [NIST], THE NIST DEFINITION OF CLOUD COMPUTING (DRAFT), SPECIAL PUBLICATION 800-145 (Draft) 2 (2011), *available at* http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (defining cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources […] that can be rapidly provisioned and released with minimal management effort or service provider interaction"); JOHN W. RITTINGHOUSE & JAMES F. RANSOME, CLOUD COMPUTING: IMPLEMENTATION, MANAGEMENT, AND SECURITY, at xxvi (2010) (defining cloud computing as "the provision of computational and storage resources as a metered service, similar to those provided by a traditional public utility company"); GERARD BLOKDIJK & IVANKA MENKEN, CLOUD COMPUTING – THE COMPLETE CORNERSTONE GUIDE TO CLOUD COMPUTING BEST PRACTICES 15 (2d ed. 2009) (describing cloud computing as "a browser-based application that is hosted on a report server"); GEORGE REESE, CLOUD APPLICATION ARCHITECTURES: BUILDING APPLICATIONS AND INFRASTRUCTURE IN THE CLOUD 2 (2009) (defining three criteria to determine whether a given service is a cloud service: (1) the service is accessible via a web browser or web services application programming interface (API); (2) zero capital expenditure is necessary to get started; and (3) you pay only for what you use as you use it).

To the extent that individuals as well as businesses increasingly rely on online service providers for data storage and processing, the level of data availability, confidentiality, and integrity offered by these providers becomes a very significant factor for information security in general.

Additionally, online services have become one of the primary threat vectors for personal computers (PCs). By making an online service deliver malicious content to its clients, attackers are able to compromise thousands of PCs within a very short time frame. The level of security offered by an online service provider therefore also has great effect on the security of client PCs.

Lastly, one particular type of online service provider has to be discussed more extensively since providers of this type collectively constitute an integral part of the Internet's logical infrastructure: Domain Name System (DNS) service providers.

On the most basic level, DNS enables the translation of domain names (e.g. example.com)[137] to IP addresses (e.g. 192.0.32.10).[138] This allows people to use names rather than difficult to remember IP addresses for identifying computers. In order to increase the number of available names and to make the task of managing those names practical,[139] DNS implements a

[137] The domain name example.com has been reserved for use in private testing and as an example in documentation materials. *See* D. EASTLAKE & A. PANITZ, RESERVED TOP LEVEL DNS NAMES, RFC 2606, at 2 (1999), ftp://ftp.rfc-editor.org/in-notes/rfc2606.txt.

[138] Note that in addition to translating domain names to IP addresses, DNS is also used, *inter alia*, to translate IP addresses to domain names (referred to as *reverse mapping*), to determine the name servers that have authority over a specific domain, or to determine the mail servers that will receive e-mails for a domain). *See* P. MOCKAPETRIS, DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION, RFC 1035 (1987), ftp://ftp.rfc-editor.org/in-notes/rfc1035.txt (defining all basic DNS record types). *Cf. also* CRICKET LIU & PAUL ALBITZ, DNS AND BIND 59, 90 (5th ed. 2006).

[139] Before the introduction of DNS, a centrally administered file (known as HOSTS.TXT) was used to provide name-to-address mappings. The administrative burden increased dramatically as the number of hosts connected

hierarchical, distributed naming system which consists of millions of name servers.[140] For example, the domain name "ny.example.com" consists of three parts: the so-called top-level domain (TLD) "com," the second-level domain "example," and the third-level domain "ny." Due to the hierarchical nature of the DNS, another second-level domain named "example" could be created under a different TLD without leading to any conflicts. There is also no need for a single central authority that maintains all domain names. DNS allows the delegation of authority for a domain (in this context more accurately referred to as a *zone*)[141] to another name server that is typically operated by the organization that is to be put in charge of that zone. Continuing the above example, the organization which has the authority over the zone ".com" will delegate the "example.com" zone to a name server operated by Example Corp. which may then decide to further delegate parts of the "example.com" zone (e.g. the zone "ny.example.com") to a name server operated by their branch office in New York.

Any computer on the Internet that needs to resolve the domain name ny.example.com uses DNS client software (referred to as a *resolver*) to first query the name server that has the authority over the ".com" zone. That name server will reply with a referral to Example Corp.'s name server to which it delegated the authority over the zone "example.com." When Example Corp.'s name server is queried, it will be able to respond with ny.example.com's IP

to the Internet grew. For a brief discussion of the history of DNS see CRICKET LIU & PAUL ALBITZ, DNS AND BIND 3 (5th ed. 2006).

[140] A name server is a computer that runs a software application that implements the DNS protocol and is configured to answer DNS queries from other computers. Popular name server software includes BIND (Berkeley Internet Name Daemon), Microsoft DNS, and Daniel J. Bernstein's djbdns.

[141] For example, the ".com" domain encompasses *all* domains that end with ".com," irrespective of which name server has the authority of these domains. The ".com" zone, on the other hand, only consists of the information which name servers have the authority over which ".com" TLDs. *Cf.* CRICKET LIU & PAUL ALBITZ, DNS AND BIND 22 (5th ed. 2006).

address (unless the zone "ny.example.com" has been further delegated).[142] However, this process does not have to be repeated every time a particular domain name needs to be resolved. All name servers implement a caching mechanism that drastically reduces the amount of queries that actually have to be performed.[143] It should also be noted that the authority over each zone is typically assigned to at least one primary and one secondary name server so as to provide redundancy.[144]

In the above example, it was simply assumed that a computer would know which name server had the authority over the ".com" zone (i.e. where to start its recursive query). However, in practice, this is not the case. In order to find the authoritative name server for any TLD zone—or to determine whether that TLD exists at all—the root name servers have to be queried. There currently are 13 root name servers[145] which collectively provide the *root zone* which solely consists of the information which name servers have been delegated authority over which TLD zones. The authority over the content of the root zone rests with IANA which is operated by the Internet Corporation for Assigned Names and Numbers (ICANN).[146]

[142] *Cf. id.* at 27 et seq.

[143] Note that, in principal, the authoritative name server—and not the resolver—determines how long DNS information is being cached by setting an appropriate time-to-live (TTL) value for each zone. *See* P. MOCKAPETRIS, DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION, RFC 1035, at 10 (1987), ftp://ftp.rfc-editor.org/in-notes/rfc1035.txt. A typical TTL value is 86400 seconds (24 hours).

[144] *Cf.* CRICKET LIU ET AL., DNS ON WINDOWS SERVER 2003, at 25 (2003).

[145] The following organizations each operate a root name server: VeriSign, Inc. (operating two root name servers), University of Southern California, Cogent Communications, University of Maryland, National Aeronautics and Space Administration (NASA), Internet Systems Consortium, Inc. (ISC), U.S. Defense Information Systems Agency, U.S. Army Research Laboratory, Autonomica Ab, RIPE NCC, ICANN, and Widely Integrated Distributed Environment (WIDE) Project. Each of the root name servers comprises multiple physical servers so as to provide redundancy. For the authoritative list of root name servers see ftp://ftp.rs.internic.net/domain/db.cache (last accessed Feb. 10, 2011).

[146] ICANN is a private not-for-profit corporation operating under a contract with the U.S. government. *Cf. Commission Communication on Internet governance: the next steps*, at 6, COM (2009) 277 final (June 18, 2009). In the 1990s, the formal authority over the root zone was the subject of significant conflict between the "founders" of the Internet (in particular the late Jon Postel) and the U.S. government. *Cf.* JACK GOLDSMITH &

Currently there are 255 country-code TLDs (ccTLDs) such as ".us," or ".eu" and 21 operational generic TLDs (gTLDs) such as ".com" or ".org."[147] The authority over TLD zones is delegated to so-called *registries* (sometimes also referred to as Network Information Centers, or NICs) which may be for-profit or non-profit organizations.[148] However, it should be noted that individuals or businesses wishing to register a domain name under a certain TLD (referred to as *registrants*) typically do not deal with the registry itself but with a *registrar* that has been accredited by the registry for the purpose of facilitating changes to the registry's TLD zone.

DNS in general but especially the name servers that have the authority over the root zone or any TLD zone have to be considered a vital part of the Internet's communications infrastructure.

2.3.3. Software Manufacturers

Software is at the core of all electronic information processing. The entities that manufacture software are therefore essential players in the information security landscape.

Most software used today is standard software that is configured according to the customer's needs. To meet the specific requirements of each customer, software manufacturers implement a great range of features. However, additional features are also implemented for

TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 29 et seq., 168 et seq. (2006). At least since the United Nation's World Summit on the Information Society (WSIS) in 2005, the conflict over the control over the root zone is much more one between different national governments (in particular the U.S. and the EU) than between the private and the public sector. *See id.* at 171.

[147] *See* http://www.iana.org/domains/root/db/ (last accessed Feb. 10, 2011).

[148] For example, the ccTLD zone ".eu" has been delegated to EURid (European Registry of Internet Domain Names) which is a private, not-for-profit organization under Belgian law. The gTLD zones ".com" and ".net," on the other hand, have been delegated to the for-profit company VeriSign, Inc.

marketing purposes and to justify new major releases of the software product. Studies indicate that most users rely on less than 10% of the features of common programs.[149] This dynamic, referred to as feature creep,[150] leads to more and more complex software which increases the potential for mistakes to be made and vulnerabilities to be created.[151]

An important distinction is traditionally made between open source software (OSS) and proprietary software.[152] However, this distinction is not as important for software security as it might seem. Open source software has the advantage that many people can review the source code and thereby help discovering and fixing vulnerabilities. Depending on the skills and motivation of the people involved in a specific open source project, such an open process might yield better results than the development processes of a corporation developing proprietary software. However, the fact that software has been released under an open source

[149] Cheryll Aimée Barron, *High tech's missionaries of sloppiness*, SALON.COM, Dec. 6, 2000, http://www.salon.com/technology/feature/2000/12/06/bad_computers (quoting Gary Chapman, director of the 21st Century Project at the University of Texas: “repeated experiences with software glitches tend to narrow one’s use of computers to the familiar and routine. Studies have shown that most users rely on less than 10 percent of the features of common programs”). *Cf.* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 61 (2008).

[150] *Cf., e.g.,* Charles C. Palmer, *Can We Win the Security Game?*, 2 IEEE SECURITY & PRIVACY 10, 11 (2004) (noting that “[h]aving escaped the constraints of small memory sizes and slow processor speeds, software developers seem to have little motivation to resist the rampant feature creep in today’s systems”).

[151] Note that feature creep may also occur in open source projects. *Cf.* ERIC S. RAYMOND, THE CATHEDRAL & THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY 96 (2001) (describing why the open source community typically values new features more than they value patches).

[152] All OSS licenses have, *inter alia*, the following characteristics: (1) they allow the licensee to redistribute the software free of charge, (2) they also cover the software’s source code, and (3) they allow the licensee to create and distribute derivative works. For further details see the Open Source Initiative’s Open Source Definition, *available at* http://www.opensource.org/osd.html. *Cf. also* LAWRENCE ROSEN, OPEN SOURCE LICENSING: SOFTWARE FREEDOM AND INTELLECTUAL PROPERTY LAW 2 (2004) (providing a detailed analysis of Open Source Definition).

license does not mean that anyone will actually review the source code. Accordingly, open source software cannot *per se* be considered more secure than proprietary software.[153]

Of more relevance than the fact of the software being proprietary or open source is—in particular with regard to potential responsibilities of software manufacturers—whether a manufacturer's motive is of a commercial or non-commercial nature. It has to be emphasized that commercial software is not necessarily proprietary[154] and non-commercial software is not necessarily open source.[155]

Concerning the issue of software security, manufacturers still predominantly follow a reactive approach. When offering a new type of software or new functionality, it is particularly important for a company to be the first on the market. Once a significant number of customers have adopted a particular product, switching costs[156] and network effects[157] might make it difficult for other companies to enter the market. Accordingly, software manufacturers attempt to minimize the time-to-market, focusing on those aspects of their product that will

[153] *Cf.* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 345 (2000) (criticizing the common belief that open source software is necessarily more secure).

[154] Many software manufacturers that make their product freely available under an open source license do so in order to strengthen their market position in related markets or to increase their potential customer base for commercial services such as training or consulting. *Cf.* HENRY CHESBROUGH, OPEN BUSINESS MODELS: HOW TO THRIVE IN THE NEW INNOVATION LANDSCAPE 45 (2006); ERIC S. RAYMOND, THE CATHEDRAL & THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY 134 et seq. (2001).

[155] *Cf.* LAWRENCE D. GRAHAM, LEGAL BATTLES THAT SHAPED THE COMPUTER INDUSTRY 23 (1999) (noting that the term "freeware" generally describes software that is "only free in terms of price; the author typically retains all other rights, including the rights to copy, distribute, and make derivative works from the software").

[156] For example, having to convert files from one data format to another or learning how to use a different user interface. *Cf.* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 11 (1999) (noting that users of information technology are notoriously subject to switching costs and lock-in).

[157] Network effects arise when the value one user places on a particular software depends on how many other people are using it. *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 45 (1999).

determine its success.[158] However, a product's level of security is typically not one of those factors.[159]

Since it is very difficult to test the security of a software[160]—and manufacturers have few incentives to do so—its level of security can often only be measured by examining the number of vulnerabilities that have been found in a particular software and subsequently publicly reported.[161] Before a software becomes popular, however, few hackers and vulnerability researchers will actually search for vulnerabilities in that software. This means that vulnerabilities in not yet popular software products are rarely reported, resulting in a lack of security indicators for new software products. Since the security of a new software product is not transparent to customers, software security is not a significant factor for its commercial success or failure. Accordingly, manufacturers typically will not regard software security as a major concern for them until their product—possibly containing hundreds of vulnerabilities—has achieved popularity.[162]

[158] *See* Ross Anderson & Tyler Moore, *Information Security Economics – and Beyond*, 27 ANN. INT'L CRYPTOLOGY CONF. 68, 74 (2007), *available at* http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf (stating that "winning market races is all important"). *Cf.* MICHEL J.G. VAN EETEN & JOHANNES M. BAUER, OECD, ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES, DSTI/DOC(2008)1, at 39 (2008), *available at* http://www.oecd.org/dataoecd/53/17/40722462.pdf; JARI RÅMAN, REGULATING SECURE SOFTWARE DEVELOPMENT 76 et seq. (2006).

[159] *See* Ross Anderson, *Why Information Security is Hard – An Economic Perspective*, 17 ANN. COMPUTER SECURITY APPLICATIONS CONF. 358, 359 (2001) (noting that these network effects lead to a philosophy that can be described as "we'll ship it on Tuesday and get it right by version 3"); ADAM SHOSTACK, AVOIDING LIABILITY: AN ALTERNATIVE ROUTE TO MORE SECURE PRODUCTS 1 (FOURTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, WORKING PAPER, 2005), *available at* http://infosecon.net/workshop/pdf/44.pdf ("If customers can't distinguish between a secure and an insecure product, the company that produces an insecure product will get to market first, and have an advantage. This shifts the high cost of dealing with insecurities to customers, who are in a poor position to fix the products they have purchased."). *Cf. also* NAT'L RESEARCH COUNCIL, TRUST IN CYBERSPACE 194 (Fred B. Schneider ed., 1999).

[160] *See infra* chapter 2.4.3 (discussing the challenges associated with measuring security).

[161] *Cf.* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 88 (2008).

[162] *Cf. id* at 56 (noting that "because latent [software] defects remain hidden until the software achieves a certain level of popularity, such defects play no role in the software manufacturer's competition to become popular").

At that point, however, the software will already be installed on thousands if not millions of their customers' computers. In such a situation, software manufacturers rarely re-develop their product with an emphasis on security.[163] They rather concentrate on issuing security updates (often referred to as *patches*) for newly reported vulnerabilities.[164] Typically, this does not reduce their competitiveness because customers have become used to having to install patches for newly discovered vulnerabilities and might also be discouraged from changing to a different product by switching costs and network effects.[165]

It is important to recognize that this reactive approach to software security puts a significant burden on customers who have to install patches in a timely fashion.[166] Some software manufacturers have therefore implemented automatic update features. Customers nevertheless

Cf. also MICHEL J.G. VAN EETEN & JOHANNES M. BAUER, OECD, ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES, DSTI/DOC(2008)1, at 39 (2008), *available at* http://www.oecd.org/dataoecd/53/17/40722462.pdf (stating that "[t]he predominant view seems to be that software markets do not reward security").

[163] To some extent, Windows Vista constitutes an exception to this rule. Microsoft has adopted a software development process that puts a very strong emphasis on security. *See* MICHAEL HOWARD & STEVE LIPNER, THE SECURITY DEVELOPMENT LIFECYCLE: SDL: A PROCESS FOR DEVELOPING DEMONSTRABLY MORE SECURE SOFTWARE (2006).

[164] Critics refer to this process as "penetrate and patch." *Cf.* JOHN VIEGA & GARY MCGRAW, BUILDING SECURE SOFTWARE: HOW TO AVOID SECURITY PROBLEMS THE RIGHT WAY 15 (2001); ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 885 (2d ed. 2008).

[165] *Cf.* Douglas A. Barnes, Note, *Deworming the Internet,* 83 TEX. L. REV. 279, 295 (2004) and DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 56 (2008) (arguing that software manufacturers might also actually profit from the fact that users rely on patches: by refusing to issue any further patches for earlier versions of their software, they can effectively eliminate these earlier versions from the market which might otherwise inhibit the acceptance of newer versions of the software). *But see* Johannes M. Bauer & Michel J.G. van Eeten, *Cybersecurity: Stakeholde rincentives, externalities, and policy options*, 33 TELECOMM. POL'Y 706, 712 (2009) (not considering the users' dependence on security patches as an advantage for the software manufacturer).

[166] It is often argued that fixing security vulnerabilities after a software has been released is much more expensive for the manufacturer than fixing them during the design, implementation, or testing phase. *See* MARK G. GRAFF & KENNETH R. VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES 55 (2003); MICHEL J.G. VAN EETEN & JOHANNES M. BAUER, OECD, ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES, DSTI/DOC(2008)1, at 42 (2008), *available at* http://www.oecd.org/dataoecd/53/17/40722462.pdf. However, most of the cost associated with patching is actually born by the customers. *See* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 57 (2008).

still face the problem that patches may break compatibility with other software products or introduce new unwanted features.[167]

2.3.4. Other Businesses, in Particular in Their Capacity as Personal Information Controllers

Businesses other than those discussed above also play a pivotal role in the information security landscape. This is primarily because they store and process vast amounts of information. This information can be broadly categorized as (1) information relating to the business's (potential) customers, (2) information relating to its employees, or (3) all other information, in particular information relating to the business itself and its internal processes.

The first category—information relating to customers—has increased drastically since the introduction of automated processing capabilities and is expected to continue to grow because it enables the following business practices: (1) targeted advertising, (2) price discrimination, and (3) credit granting.

Targeted advertising attempts to address the problem that many people who receive an advertisement are not at all interested in it, rendering the business's expenditures for reaching this individual moot. To increase the probability that a person will respond to a particular advertisement, the advertiser needs to have information about the person's interests and needs. The more detailed the information is, a business has about its (potential) customers, the better it will be positioned to maximize the effectiveness of its marketing campaigns. This

[167] *Cf.* ROSS ANDERSON ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET 5 (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport (recommending to the European Commission that software manufacturers should be required to keep patches separate from feature updates).

creates a very significant incentive for businesses to maintain vast amounts of data about consumers as well as corporate customers.[168]

The second business practice to discuss here is price discrimination, i.e. to charge different prices to various customers for the same goods or services.[169] Businesses have strong incentives to price discriminate if there are some customers who are able and willing to pay more than other customers. For example, if a company's product is worth $10 to 50 customers and $5 to another 50 customers, what should the product be sold for? If the sales price is set at $5, the company's revenue will be $500 (both groups would buy). If the price is set at $10, it will also be $500 (only the first group would by). However, if the company manages to sell the product for $10 to the first 50 and for $5 to the other 50 customers, it would have a revenue of $750. While overt price discrimination is sometimes faced with severe public criticism,[170] covert price discrimination (e.g. in the form of bundling or a customer loyalty program) is practiced extensively and rarely leads to customer opposition.[171]

[168] *Cf.* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 155 et seq. (2000); PETER SCHAAR, DAS ENDE DER PRIVATSPHÄRE: DER WEG IN DIE ÜBERWACHUNGSGESELLSCHAFT [THE END OF PRIVACY: THE WAY INTO THE SURVEILLANCE SOCIETY] 186 et seq. (2007).

[169] *See* Andrew Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet, in* ECONOMICS OF INFORMATION SECURITY 187, 203 (L. Jean Camp & Stephen Lewis eds., 2004) (identifying price discrimination as one of the main motivators for the private sector to reduce privacy). Price discrimination is one of the basic concepts in microeconomics. *See generally* LOUIS PHLIPS, THE ECONOMICS OF PRICE DISCRIMINATION (1983); Hal R. Varian, *Differential Pricing and Efficiency*, 1 FIRST MONDAY (1996), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/473/394.

[170] *Cf.* Andrew Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet, in* ECONOMICS OF INFORMATION SECURITY 187, 203 (L. Jean Camp & Stephen Lewis eds., 2004) (discussing the public revolt against discriminatory railroad pricing in the last third of the 19th century); Anita Ramasastry, *Web sites change prices based on customers' habits*, CNN.COM, June 24, 2005, http://edition.cnn.com/2005/LAW/06/24/ramasastry.website.prices/ (noting that, in September 2000, Amazon.com outraged some customers when its price discrimination practices were revealed).

[171] *See* JOSEPH TUROW ET AL., UNIVERSITY OF PENNSYLVANIA, ANNENBERG PUBLIC POLICY CENTER, OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE (2005), *available at* http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/Turow_APPC_Report_WEB_FINAL.pdf (finding that 64% of American adults who have used the Internet recently do not know it is

Businesses that sell a product or service that has very low marginal costs are particularly incentivized to employ price discrimination. In particular the marginal costs of information goods such as electronic content or software that can be downloaded over the Internet are effectively $0.[172] This means that reducing the price from $400 to $40 for a customer group that would not have otherwise acquired the product, still results in a profit of $40 per transaction. This is, of course, only possible if there is no market for used goods. As regards information goods, this market has been strongly suppressed by a combination of legal and technical means.[173]

To be able to practice price discrimination, the seller needs to have at least some idea of what a particular customer is willing to pay.[174] The traditional way to address this challenge is to offer different versions of the same product, tailoring each version to a particular customer group (e.g. hardcover vs. paperback editions of books).[175] However, versioning is not always possible and will necessarily not be as effective as individualized price discrimination.

legal for "an online store to charge different people different prices at the same time of day"; 71% don't know it is legal for an offline store to do that).

[172] *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 21 (1999).

[173] Businesses "license" rather than "sell" information goods, thereby circumventing the first-sale doctrine of copyright law, making the sale of a "used" information good an illegal distribution of a copyrighted work. *See* Vernor v. Autodesk, Inc., 621 F.3d 1102, 1111 (9th Cir. 2010) (holding that "a software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions"; as a licensee, Vernor was not entitled to invoke the first sale doctrine); Bundesgerichtshof [BGH] [Federal Court of Justice] Feb. 3, 2011, I ZR 129/08 (F.R.G.) (making a referral for a preliminary ruling to the ECJ regarding the question of whether a user who has purchased a "used" software has the right to run the software—and thereby copy it into the computer's memory—under Parliament and Council Directive 2009/24, art. 5(1), 2009 O.J. (L 111) 16, 18 (EC) which grants a "lawful acquirer" the right to use software "in accordance with its intended purpose"). By employing digital rights management (DRM) systems, the transfer of information goods from one customer to another is further complicated by technical means.

[174] *Cf.* HAL R. VARIAN ET AL., THE ECONOMICS OF INFORMATION TECHNOLOGY: AN INTRODUCTION 14 (2004).

[175] *Cf.* Hal R. Varian, *Versioning Information Goods, in* INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL INFORMATION AND INTELLECTUAL PROPERTY 190 (Brian Kahin & Hal R. Varian eds., 2000).

Similar to targeted advertising, this creates a situation where the more information a business obtains about its customers, the better it will be able to maximize its profits.

The third business practice resulting in a need for customer data is credit granting. In particular in the U.S., many businesses are willing to grant credit to their customers, most commonly consumers. To know which consumers to offer credit to and to be able to offer credit terms that correspond to the individual consumer's risk of default—strictly speaking a form of price discrimination—a consumer's creditworthiness has to be determined. In the U.S. as well as in the EU, creditors usually do not attempt to perform this determination themselves but rather turn to consumer reporting agencies for that purpose.[176] In the U.S., there are only three national consumer reporting agencies[177] while in the EU, each Member State has its own credit reporting system.[178] To be able to assess a consumer's creditworthiness, a consumer reporting agency needs various types of personal information about each consumer, including a consumer's credit history, employment history, marital status, and place of residence. This creates a situation where credit reporting agencies have an incentive to obtain—and credit granting businesses in general have an incentive to provide to them—as much information as possible about each consumer.

[176] *Cf.* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 24 et seq. (2000); PETER SCHAAR, DAS ENDE DER PRIVATSPHÄRE: DER WEG IN DIE ÜBERWACHUNGSGESELLSCHAFT [THE END OF PRIVACY: THE WAY INTO THE SURVEILLANCE SOCIETY] 194 et seq. (2007).

[177] *Cf.* Fair Credit Reporting Act § 603(p), 15 U.S.C. § 1681a(p) (defining the term "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis"). These are Equifax Inc., Experian plc, and Trans Union, LLC.

[178] In some Member States, there is only a single public consumer reporting agency (e.g. in France) while in others, there are private as well as public agencies (e.g. Germany) or only private agencies (e.g. the U.K.). *Cf.* NICOLA JENTZSCH, FINANCIAL PRIVACY: AN INTERNATIONAL COMPARISON OF CREDIT REPORTING SYSTEMS 89, 95, 101 (2d ed. 2007).

These three very profitable business practices described above (targeted advertising, price discrimination, and credit granting) practically guarantee that businesses will continue to amass vast amounts of personal information about their (potential) customers.[179] Cheap storage and processing capabilities enable these practices and continuously improving data mining techniques will allow businesses to extract more and more value from personal information,[180] providing additional incentives for collecting this type of information in the first place.

The second type of information all businesses maintain is information relating to their employees. This type of information is, however, typically not as profitable for businesses as customer information. Accordingly, businesses typically only maintain employee information—beyond what is legally required—to the extent that it is needed for performance evaluations, social security, and accounting purposes. The integrity and availability of that information is nevertheless of significant value to an organization. Furthermore, its confidentiality is of great concern to employees.

The third type of information covers all other information that is maintained by a business, in particular information relating to the business itself and its internal processes. What is characteristic for this type of information is that its confidentiality, integrity, and availability

[179] Note that technological "solutions" such as "privacy-enhancing technologies" (PETs) cannot alleviate this need for personal information. *Cf. Commission Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, at 3, COM (2007) 228 final (May 2, 2007) (defining PET as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system").

[180] *Cf., e.g.,* ANTONIOS CHORIANOPOULOS & KONSTANTINOS TSIPTSIS, DATA MINING TECHNIQUES IN CRM: INSIDE CUSTOMER SEGMENTATION (2009). *Cf. also* David Lyon, *Surveillance as social sorting: computer codes and mobile bodies, in* SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK AND AUTOMATED DISCRIMINATION 13, 20 (David Lyon ed., 2003).

is primarily only of value to the business itself. A significant exception, however, is the information publicly traded companies have to disclose to the public. The integrity (i.e. accuracy) of such information is primarily not in the interest of the business but in the interest of the (potential) shareholders.

2.3.5. Consumers

Consumers primarily act in the information security landscape by deciding which Internet access providers and online service providers to use, which businesses to trust their personal information with, and by choosing certain software for their own PCs. Collectively, this gives consumers a significant power over the industry. However, this power can only be exerted to improve information security to the extent that the level of information security offered by a particular provider, manufacturer, or general business is transparent to the consumer.[181]

The choices consumers make in this regard do not only affect themselves. In particular their choices regarding the software they use on their own PCs are of significance to all other entities connected to the Internet. If a PC is compromised due to a vulnerability in a software the consumer chose to install on his PC, that PC is typically used to further attack other computers.[182] In addition to the choice of software, the diligence with which consumers configure the software, install patches, and implement other security measures such as a firewall or anti-malware software also greatly affects the security of their PCs and, by extension, the probability that their PCs will become a threat to other computers connected to the Internet.

[181] *Cf.* chapter 2.4.3.

[182] *Cf. infra* chapter 7.4.2 (discussing botnets).

2.3.6. Governments

Governments are not only a significant actor in the information security landscape due to their regulatory powers but also due to the fact that they too store and process vast amounts of personal information. They do so in order to facilitate the administration of government services (e.g. social security or pensions) or other government functions (e.g. taxation or regulatory oversight).[183]

2.3.7. Malicious Actors

In an organizational context, malicious actors can generally be classified as either insiders or outsiders with respect to the attacked organization. While the insider threat is traditionally estimated to be more significant than the outsider threat, no evidence exists to support this assumption.[184]

Specifically regarding computer security, malicious actors are traditionally categorized either as hackers or script kiddies. The term "hacker," while originally only used for non-malicious actors who "[enjoy] learning the details of computer systems and how to stretch their

[183] *Cf.* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 13 (2000) (discussing some of the incentives for governments to collect vast amounts of personal information). *Cf. also* PETER SCHAAR, DAS ENDE DER PRIVATSPHÄRE: DER WEG IN DIE ÜBERWACHUNGSGESELLSCHAFT [THE END OF PRIVACY: THE WAY INTO THE SURVEILLANCE SOCIETY] 96 et seq. (2007).

[184] *Shostack* and *Stewart* have traced the often cited claim that 70% of all incidents are caused by insiders to the following Gartner Research report which draws its conclusions from the fact that "[t]wo recent cases show that insiders—not outside cyberattacks—are responsible for most incidents that cause real losses." JOHN PESCATORE, GARTNER, HIGH-PROFILE THEFTS SHOW INSIDERS DO THE MOST DAMAGE, FT-18-9417 (2002), *available at* http://www.gartner.com/resources/111700/111710/111710.pdf. *See* ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 49, 181 (2008) (stating that "we were unable to find *any* credible evidence in support of the claim that 70% of all incidents are caused by insiders"). Recent evidence suggests that the majority of incidence might actually be caused by outsider. *See* WADE BAKER, VERIZON, 2010 DATA BREACH INVESTIGATIONS REPORT 12 (2010), *available at* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf (stating that 70% of all breaches examined by the Verizon RISK Team and the United States Secret Service were caused by external threat agents).

capabilities,"[185] came to denote people who have deep technical knowledge and very advanced programming skills which they use to discover and exploit security vulnerabilities in computer software. The term "script kiddy," on the other hand, refers to an individual, typically in his teenage years, who does not possess the skills to discover and exploit vulnerabilities by himself but rather uses ready-to-run scripts (or other tools) to exploit a known vulnerability.[186] Due to the high availability of powerful and easy to use hacker tools, such individuals can also mount significant threats.

However, the days when malicious actors were individuals mostly motivated by fame and glory—only occasionally seeking fortune—are long gone. Breaking into computer systems and subsequently exploiting their resources and the information they store and process has become a business—and a very profitable one.[187] The field of malicious actors is therefore dominated by criminal organizations,[188] regular businesses performing corporate espionage,[189] or state actors pursuing economic and national security interests[190] by attacking computer systems that are within or outside their jurisdiction.[191]

[185] *See* ERIC S. RAYMOND, ET AL., THE NEW HACKER'S DICTIONARY 233 (1996), *Cf. also* STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 39 (1984) (describing the "hacker ethic").

[186] *Cf.* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 44 (2000).

[187] *Cf.* EUROPOL, THREAT ASSESSMENT (ABRIDGED): INTERNET FACILITATED ORGANISED CRIME 5 (2011), *available at* http://www.europol.europa.eu/publications/Serious_Crime_Overviews/Internet%20Facilitated%20Organised%20Crime%20iOCTA.pdf (describing the "digital underground economy" as sophisticated and self-sufficient).

[188] *Cf. id.*; ROSS ANDERSON ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET 9 (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport (dating the start of the "online criminal revolution" to 2004).

[189] *Cf.* SHANE W. ROBINSON, CORPORATE ESPIONAGE 201, at 6 (2007), *available at* http://www.sans.org/reading_room/whitepapers/engineering/corporate-espionage-201_512 (documenting a number of high-profile cases). *Cf. also* Richard Power, *Corporate Espionage: Tomorrow Arrived Yesterday*, CSOONLINE.COM, Feb. 26, 2010, http://www.csoonline.com/article/558021/corporate-espionage-tomorrow-arrived-yesterday.

[190] *Cf., e.g.,* Rhys Blakely et al., *MI5 alert on China's cyberspace spy threat*, TIMES, Dec. 1, 2007, *available at* http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece; Joseph Fitchett,

This is not to say, that politically motivated attacks—whether carried out by individuals or a state actor—or acts of vandalism by disgruntled employees pose no threat to information security. A number of recent high-profile events fall into the former category: In April 2007, very effective distributed denial of service (DDoS) attacks[192] were launched against the websites of the Estonian government, the Estonian parliament, Estonian banks, and news organizations after Estonia had relocated a statue dedicated to fallen soldiers of the former Soviet Union.[193] In August 2008, one day after the Russian Federation invaded Georgia, massive DDoS attacks were launched against high-profile Georgian websites.[194]

In recent years, "cyber terrorists" have often been said to constitute a very important group of malicious actors online.[195] However, not a single act of "cyber terrorism" has so far been

French Report Accuses U.S. of Industrial Sabotage Campaign, N.Y. TIMES, July 19, 1995, *available at* http://www.nytimes.com/1995/07/19/news/19iht-rivals.html?pagewanted=1.

[191] If the U.S. or an EU Member State found itself at war with another state that has developed sufficient cyber attack capabilities, the role of state actors would become significantly more important. *Cf., e.g.,* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 180 et seq. (2010) (theorizing about a cyber war between the U.S. and China). *Cf. also* Elihu Zimet & Charles L. Barry, *Military Service Overview, in* CYBERPOWER AND NATIONAL SECURITY 285, 300 (Franklin D. Kramer et al. eds., 2009) (describing the cyber programs of the various service branches of the United States Armed Forces).

[192] DDoS attacks are typically carried out by using a network of compromised computers (referred to as a botnet) to consume all bandwidth or resources of the targeted system, thereby denying its service to legitimate users. *See infra* chapter 7.4.2 (discussing botnets in greater detail).

[193] *See* JEFFREY CARR, INSIDE CYBER WARFARE 3 (2009).

[194] *See id.* at 15. *See also* PETER SOMMER & IAN BROWN, OECD, REDUCING SYSTEMIC CYBERSECURITY RISK, IFP/WKP/FGS(2011)3, at 58 (2011), *available at* http://www.oecd.org/dataoecd/3/42/46894657.pdf (questioning whether such an attacks justifies the label "cyberwar"). *Cf. infra* chapter 7.4.1 (discussing the "attribution problem"—the difficulty of identifying an attacker).

[195] *Cf., e.g.,* Joel P. Trachtman, *Global Cyberterrorism, Jurisdication, and International Organization, in* THE LAW AND ECONOMICS OF CYBERSECURITY 259, 259 (Mark F. Grady & Francesco Parisi eds., 2006) (asserting that Al Qaeda had "developed an academy of cyberterrorism" and citing Barton Gellman, *Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say*, WASH. POST, June 27, 2002, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711_pf.html which indeed does not provide any basis for this assertion).

committed against the EU or the U.S.[196] and many experts rightly question whether the threat of "cyber terrorism" is as serious as often portrayed in the media.[197]

In particular, it should be pointed out that attacks on the security of information and information systems only have the potential to create terror (i.e. fear) if not just the information itself but people and their livelihoods are threatened.[198]

Note that this thesis occasionally uses the term "attacker" to refer to a malicious actor, whether it is an individual, corporation, or state actor.

2.4. Fundamental Challenges in the Field of Information Security

Any regulatory attempt to improve the current state of information security has to be considered in light of the fundamental challenges identified below. Some of these challenges can be directly addressed by regulatory means while others are largely outside the influence of any regulatory policy. The recognition of both types of challenges is essential for the

[196] *See* Irving Lachow, *Cyber Terrorism: Menace or Myth?, in* CYBERPOWER AND NATIONAL SECURITY 437 (Franklin D. Kramer et al. eds., 2009).

[197] For example, in February 2010, the Bipartisan Policy Center's cyber attack simulation "Cyber Shockwave" was based on the premise that a botnet attack would escalate into power failures, millions of cell phones without service and Wall Street shut down for a week. This simulation was widely covered in the media, in particular by CNN which twice aired the hour-long special "Cyber ShockWave: We Were Warned." *See also,* Ellen Nakashima, *War game reveals U.S. lacks cyber-crisis skills*, WASH. POST, Feb. 17, 2010, at A3, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/16/AR2010021605762.html. However, experts highly doubted the simulation's value. One stated that he was "highly sceptical that a botnet attack could easily escalate into power failures, disruption of cell service for millions, and Wall St getting shut down for a week. (Anyone who claims the latter doesn't appear to understand how the New York Stock Exchange works) […]. Simulations should be credible, or they're just propaganda." *See Cyber Attack Simulation Underscores Areas of Policy Weakness*, SANS NEWSBITES (SANS Institute, Bethesda, Md.), Feb. 19, 2010, http://www.sans.org/newsletters/newsbites/newsbites.php?vol=12&issue=14#sID201. *Cf. also* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 135 (2010) (stating that cyber terrorism "is largely a red herring and, in general, the two words 'cyber' and 'terrorism' should not be used in conjunction").

[198] *Cf.* Irving Lachow, *Cyber Terrorism: Menace or Myth?, in* CYBERPOWER AND NATIONAL SECURITY 437, 448 (Franklin D. Kramer et al. eds., 2009) (stating that "[h]istory shows that the majority of cyber attacks, even viruses that cause billions of dollars of damage to an economy, are not going to cause the levels of fear and/or horror desired by most terrorists. Even the temporary disablement of a component of a critical infrastructure may not cause the desired emotions.").

assessment of currently implemented regulatory policies as well as the development of new policies.

2.4.1. The Imperfection of Technology

To create any technological product that behaves exactly as expected, is a very challenging undertaking—even for the simplest of products. Software products, however, are all but simple. Their complexity brings with it, various types of errors (referred to as *bugs*), a significant amount of which constitute security vulnerabilities. During the development of a software, vulnerabilities can be introduced at the architectural level,[199] the design level,[200] or the implementation level.[201] This leaves plenty of opportunities for software developers to make mistakes which automated tools are often not able to detect—in particular if the mistakes are introduced at the architectural or design level.[202] Even renowned experts for secure software development estimate that there is roughly one security bug per 1,000 lines in

[199] For example, the mail server software Sendmail—in violation of the principles of separation of duties and least privilege—implements a monolithic architecture that makes it very difficult to truly separate different functions from one another and only grant them the least privileges needed. Other mail server software—in particular Postfix and qmail—specifically avoid the vulnerabilities associated with a monolithic architecture. *See* KYLE D. DENT, POSTFIX: THE DEFINITIVE GUIDE 7 (2003); JOHN R. LEVINE, QMAIL 10 (2004).

[200] For example, in November 2009 a flaw was discovered in the design of the Transport Layer Security (TLS) protocol and Secure Socket Layer (SSL) protocol (CVE-2009-3555). It allowed cryptographic parameters to be renegotiated at the client's request without verifying the request's authenticity, thereby creating a vulnerability that could be exploited to compromise the confidentiality and integrity of the communication. To fix this vulnerability, the standard describing TLS had to be updated and subsequently implemented in all software products using TLS/SSL. *See* E. RESCORLA, TRANSPORT LAYER SECURITY (TLS) RENEGOTIATION INDICATION EXTENSION, RFC 5746 (2010), ftp://ftp.rfc-editor.org/in-notes/rfc5746.txt.

[201] The most common implementation level vulnerabilities are buffer overflows. *See* MARK G. GRAFF & KENNETH R. VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES 30, 55, 99 (2003) (describing architecture, design, and implementation level vulnerabilities).

[202] *See* GARY MCGRAW, SOFTWARE SECURITY: BUILDING SECURITY IN 22 (2006) (noting that automated tools are only able to discover the most basic vulnerabilities and are therefore suitable to demonstrate that a software is very unsecure—but unsuitable to demonstrate the opposite).

their source code.[203] Furthermore, evidence suggests that the number of security-related bugs grows exponentially with a software's complexity.[204] The continuous growth of software complexity—largely caused by feature creep discussed *supra* in chapter 2.3.3—is therefore particularly worrisome. For example, Windows NT 3.1 had approximately 3 million lines of code while Windows NT 3.5 had 10 million, Windows NT 4 16.5 million, Windows 2000 29 million, Windows XP 45 million, and Windows Vista 55 million lines of code.[205] The Linux kernel has seen a similar growth from 1.6 million lines of code in version 2.2.0 to 3 million in version 2.4.0, 5.2 million in version 2.6.0 and 11.5 million in the currently stable version 2.6.34.[206]

The security of software could be significantly improved by educating software developers about security issues and integrating security into the software development process from the very start. A few software manufacturers, most notably Microsoft,[207] have adopted more secure software development processes that promise to significantly reduce the number of

[203] *See* MARK G. GRAFF & KENNETH R. VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES 5 (2003). *Cf.* STEVE MCCONNELL, CODE COMPLETE: A PRACTICAL HANDBOOK OF SOFTWARE CONSTRUCTION 521 (2d ed. 2004) (stating that the industry average is 1 to 25 errors per 1000 lines of code for delivered software).

[204] *See* GARY MCGRAW, SOFTWARE SECURITY: BUILDING SECURITY IN 10 et seq. (2006); ERIC STEVEN RAYMOND, THE ART OF UNIX PROGRAMMING 85 (2003).

[205] *See* ROBERT COWART & BRIAN KNITTEL, MICROSOFT WINDOWS VISTA IN DEPTH 9 (2008). Note that Microsoft did not release any numbers for Windows 7.

[206] The source code of the Linux kernel is available at http://www.kernel.org/pub/linux/kernel/ (last accessed June 15, 2010). The numbers of lines of code were calculated by only considering C source code files (*.c) and C header files (*.h).

[207] Microsoft has developed its own software development process coined Security Development Lifecycle (SDL). *See* MICHAEL HOWARD & STEVE LIPNER, THE SECURITY DEVELOPMENT LIFECYCLE: SDL: A PROCESS FOR DEVELOPING DEMONSTRABLY MORE SECURE SOFTWARE 27 et seq. (2006) (discussing the history of SDL at Microsoft). *See* MICROSOFT CORP., MICROSOFT SECURITY DEVELOPMENT LIFECYCLE (SDL) – VERSION 5.0 (2010), *available at* http://www.microsoft.com/downloads/details.aspx?FamilyID=7d8e6144-8276-4a62-a4c8-7af77c06b7ac&displaylang=en.

vulnerabilities contained in a released software product.[208] However, for the reasons referred to above, the creation of bug-free software is impossible, at least for the foreseeable future.[209]

2.4.2. The Imperfection of People

Even if it were ever possible to develop and deploy technology free of any vulnerabilities—a big if—such technology would, at some point, still have to be interacted with by humans for it to be useful. Humans, however, occasionally make mistakes and will never be perfect. Indeed, they are often said to constitute the weakest link in any system.[210] This would still leave an attacker plenty of ways to compromise a technologically perfectly secure system along with the information it holds.

Besides making common mistakes like forgetting to install a certain patch or accidentally entering incorrect data into a customer database,[211] people generally exhibit two major flaws that highly impact information security: we are easily manipulated and we often perceive risks incorrectly.

The practice of manipulating people in an attempt to make them disclose confidential information or perform other actions that compromise the security of information is referred

[208] Microsoft claims to have reduced the number of vulnerabilities in newly developed code by more than 50%. *See* MICHAEL HOWARD & STEVE LIPNER, THE SECURITY DEVELOPMENT LIFECYCLE: SDL: A PROCESS FOR DEVELOPING DEMONSTRABLY MORE SECURE SOFTWARE 13 (2006).

[209] It is of course impossible to estimate if artificial intelligence might one day be able to develop bug-free software.

[210] *See* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 255 (2000); KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY 3 (2002).

[211] The issue of usability of security systems has recently become the focus of many research efforts. In particular, an annual workshop, the Symposium On Usable Privacy and Security (SOUPS) has been organized. *See* http://cups.cs.cmu.edu/soups/ (last accessed Feb. 10, 2011). For further references see ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 61 (2d ed. 2008).

to as *social engineering*.[212] It can be performed, *inter alia*, by exploiting people's willingness to help (e.g. "I've forgotten my access card, would you let me in?"), by taking advantage of sympathy or guilt, or by intimidating people.[213]

The impact human factors may have on the security of a system is particularly well demonstrated by a certain type of social engineering referred to as phishing. Phishing describes the practice of impersonating a trustworthy entity by making a website or an e-mail look as if it originated from that trustworthy entity in an attempt to make users disclose sensitive information (e.g. passwords).[214] This fundamentally constitutes an authentication problem. From a technological perspective, this problem has been solved long ago by introducing Secure Sockets Layer (SSL) and subsequently Transport Layer Security (TLS)[215] to authenticate websites and Secure/Multipurpose Internet Mail Extensions (S/MIME)[216] to authenticate the sender of an e-mail. This means for example that technological measures can provide reasonable assurance that a request for the website amazon.com will only be answered by that server. However, if a user is manipulated into visiting arnazon.com (note the "rn"), the very same technological measures would confirm the authenticity of

[212] *See, e.g.,* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY (2002); ENISA, SOCIAL ENGINEERING: EXPLOITING THE WEAKEST LINKS (2008), *available at* http://www.enisa.europa.eu/act/ar/deliverables/2008/social-engineering/at_download/fullReport.

[213] *Cf.* KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY 77, 105 (2002).

[214] *Cf.* Stephen D. Fried, *Phishing: A New Twist to an Old Game, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 2853 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007). *Cf. also* EUROPOL, HIGH TECH CRIMES WITHIN THE EU: OLD CRIMES NEW TOOLS, NEW CRIMES NEW TOOLS: THREAT ASSESSMENT 2007, at 27 (2007), *available at* http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf.

[215] *See* T. DIERKS & E. RESCORLA, THE TRANSPORT LAYER SECURITY (TLS) PROTOCOL VERSION 1.2, RFC 5246 (2008), ftp://ftp.rfc-editor.org/in-notes/rfc5246.txt.

[216] *See* B. RAMSDELL & S. TURNER, SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME) VERSION 3.2 MESSAGE SPECIFICATION, RFC 5751 (2010), ftp://ftp.rfc-editor.org/in-notes/rfc5751.txt.

communications received from that web server even though they are not authentic in the sense that they do not originate from the website the user thought he was communicating with.[217] This demonstrates why phishing cannot be solved by technological means alone.[218]

The second major flaw is incorrect perception of risks—even in situations when enough information is available about a risk's impact and probability.[219] We typically overestimate risks that are out of our control (e.g. the risk of a car accident when somebody else is driving the car or the accidental destruction of data that is stored with an external online service provider) and underestimate risks we belief are under our control (e.g. accidentally deleting valuable information ourselves).[220] We also overestimate risks associated with malicious threat agents (e.g. a hacker wiping out a hard drive) as compared to accidents (e.g. a hard disk failure).[221]

Furthermore, the heuristics we use to assess probabilities often yield incorrect results: If the probability that a certain event occurs in any given year (e.g. that one of the company's servers is compromised) is fifty percent, most people would (incorrectly) assume that it is more likely that the event occurred every second year than that the event occurred in three

[217] Note that Amazon.com, Inc. has registered arnazon.com to prevent this type of attack.

[218] As discussed *supra*, phishing is a problem of authenticating the service provider (amazon.com in the above example). Efforts to mitigate the risk of phishing by mandating improved methods for authenticating users are therefore entirely misplaced. *Cf., e.g.,* Ritu Singh, *Two-Factor Authentication: A Solution to Times Past or Present? The Debate Surrounding the Gramm-Leach-Bliley Security Safeguards Rule and the Methods of Risk Assessment and Compliance*, 2 I/S: J. L. & POL'Y FOR INFO. SOC'Y 761, 776 (2006) (discussing why two-factor authentication is ill-suited to address risks like phishing or Trojan horses).

[219] For a discussion of the challenge posed by insufficient risk-related information see chapter 2.4.3.

[220] *Cf.* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 257 (2000)

[221] *Cf.* Bruce Schneier, *The Psychology of Security*, 2008 AFRICACRYPT 50, 55 (naming further examples of how we typically overestimate certain risks and underestimate others).

consecutive years followed by three years without the event occurring.[222] People are also often risk averse in the sense that, in an experiment, they would prefer to receive an assured payment of $50 rather than a chance of 50% to win $200.[223] We also often confuse the lack of evidence for something (e.g. that a certain rare but high-impact event, a so-called "Black Swan," can occur) with evidence that it does not exist (sometimes referred to as the round-trip fallacy).[224] When calculating probabilities we often give significant weight to familiar or easily-imagined risks such as those risks that receive wide media coverage (referred to as the availability heuristic)[225] or to our recent experiences (referred to as the anchoring effect).[226] People also often overestimate the representativeness of small samples (incorrectly believing in the "law of small numbers").[227] Finally, we are often insensitive to prior probabilities: if one in one million connections constitute a network attack and an intrusion detection system has an accuracy of 99.9%—0.1% of all intrusions are missed (0.1% false negatives) and 0.1% of regular connections are incorrectly identified as intrusions (0.1% false positives)—most

[222] Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124, 1125 (1974) (discussing this phenomenon as the "[m]isconception of chance" using multiple flips of a coin). *Cf. also* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 99 (2009).

[223] Prospect theory was developed by *Tversky* and *Kahneman* to model such risk aversion. *See* Amos Tversky & Daniel Kahneman, *Prospect Theory: An Analysis of Decision under Risk*, 47 ECONOMETRICA 263 (1979).

[224] *See* NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE 52 (2007) (stating another example for a round-trip fallacy: confusing the statements "almost all terrorists are Moslems" with "almost all Moslems are terrorists"). *Cf. also id.* at xvii (explaining why the term "Black Swan" is used to describe rare but high-impact events: "[b]efore the discovery of Australia, people in the Old World were convinced that *all* swans were white [which] seemed completely confirmed by empirical evidence").

[225] *See* Bruce Schneier, *The Psychology of Security*, 2008 AFRICACRYPT 50, 64 (citing BARRY GLASSNER, THE CULTURE OF FEAR: WHY AMERICANS ARE AFRAID OF THE WRONG THINGS (1999)).

[226] *See* Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124, 1128 (1974); Gretchen B. Chapman & Eric J. Johnson, *Incorporating the Irrelevant: Anchors in Judgments of Belief and Value, in* HEURISTICS AND BIASES: THE PSYCHOLOGY OF INTUITIVE JUDGMENT 120 (Thomas Gilovich et al. eds., 2002).

[227] *See* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 100 (2009); Amos Tversky & Daniel Kahneman, *Belief in the law of small numbers, in* JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES 23 (Daniel Kahneman et al. eds., 1982).

people would assume that the probability that a connection identified by the system as an intrusion actually constitutes an attack is 99.9% even though it is only 0.1% (this is referred to as the base rate fallacy).[228]

In addition to often making incorrect assessments of risks, most people also tend to be very overconfident with regard to the accuracy of their assessments.[229] This is a phenomenon that is particularly strong among successful managers who infer from their success that they are very good at what they do. However, in many cases, their success is not the product of their exceptional skills but rather pure luck. For example, it was shown that *Manfred Albrecht Freiherr von Richthofen* (the "Red Baron") who is credited with far more air combat victories than any other pilot during World War I might only have been lucky but not exceptionally skilled. Given the number of pilots and the win ratio, there was a probability of 30% that, by luck alone, one pilot would win 80 air combat victories—the number *von Richthofen* is credited for.[230] Similarly, many "successful" (risk) managers might also have been rather lucky than exceptionally skilled.[231]

[228] Note that, in the above example, the 0.1% false positive rate results in 1000 false alarms for every actual intrusion. For further discussion of the base rate fallacy see, for example, DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 101 (2009); Bruce Schneier, *Why Data Mining Won't Stop Terror*, WIRED, Mar. 9, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/03/70357, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 9, 11 (2008) (discussing how the base rate fallacy might lead to the erroneous conclusion that data mining is suitable for identifying terrorists).

[229] *See* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 102 et seq. (2009). *Cf. also* Francesca Giardini et al, *Overconfidence in Predictions as an Effect of Desirability Bias, in* ADVANCES IN DECISION MAKING UNDER RISK AND UNCERTAINTY 163 (Mohammed Abdellaoui & John D. Hey eds., 2008) (demonstrating that overconfidence in predictions is related to the desirability of the predicted outcome).

[230] *See* M. V. Simkin & V. P. Roychowdhury, *Theory of Aces: Fame by Chance or Merit?*, 30 J. OF MATHEMATICAL SOC. 33 (2006).

[231] *See* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 110 (2009) (raising the question to which extent success in management can be compared to winning a coin-flipping tournament).

The imperfections of people with regard to information security and specifically the assessment of risks can be remedied to some extent by training and better education.[232] They nevertheless pose a serious challenge for the security of any information system[233] as well as for risk management in general, whether it is performed by a policy maker, a manager of a private corporation, or a consumer.

2.4.3. Uninformed Risk Decisions and the Difficulty of Measuring Security

By acquiring certain products or using certain services, individuals and organizations alike, make risk decisions. However, these decisions are often made without the benefit of reliable information about the security properties of a product or service.[234] This is mostly due to two reasons: First, security-related information is often not disclosed by manufacturers and service providers.[235] Second, the information that is publicly available is often perceived to be insufficient to measure the security properties of products and services.

[232] Information security awareness training and education is commonly considered a best practice for all organizations. *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, ISO/IEC 27002:2005 § 8.2.2 (2005). *Cf.* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 57 et seq. (2d ed. 2010); DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 203 (2009) (stating that most heuristic biases can be corrected by calibration training, mostly consisting of repetition and feedback). For further information regarding calibration see Sarah Lichtenstein et al., *Calibration of probabilities: The state of the art to 1980, in* JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES 306 (Daniel Kahneman et al. eds., 1982).

[233] *See generally* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 255 (2000); ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 24 (2d ed. 2008).

[234] *Cf.* ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 147 et seq. (2008) (noting that the "pursuit of objective data about real-world outcomes" is necessary "to enable better security decision-making" because "[g]athering, analyzing, and acting on the lessons of objective data is the only way for information security to become a science not only in its academic aspects, but also in how it is used on a day-to-day bases"). *Cf. also* NAT'L RESEARCH COUNCIL, TRUST IN CYBERSPACE 184 et seq. (Fred B. Schneider ed., 1999).

[235] *Cf. generally* ROSS ANDERSON ET AL, SECURITY ECONOMICS AND THE INTERNAL MARKET 26 (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport (stating that "[t]here has for many years been a general lack of adequate statistics on information security" and that "[t]he

As regards the first issue, few software manufacturers voluntarily disclose any information that could be used to measure the security of their products.[236] For example, Microsoft is one of very few commercial manufacturers which have at least disclosed information about their software development process.[237] Internet access providers typically do not disclose the level of availability they were able to provide in the past even tough it might be very valuable for a potential customer to know that, e.g., the average downtime for a customer of a certain provider was five hours per year as compared to ten hours per year at a different provider.[238] Similarly, online service providers and businesses in general usually do not disclose information regarding the availability, confidentiality, or integrity of the information they store for their customers[239]—unless they are compelled to do so by law.[240]

available data are insufficient, fragmented, [and] incomparable"); ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 75 (2008) (noting that "[a] core aspect of scientific research—the ability to gather objective data against which to test hypotheses—has been largely missing from information security"); ANDREW JAQUITH, SECURITY METRICS: REPLACING FEAR, UNCERTAINTY, AND DOUBT 10 (2007) (arguing that formal security measurement is necessary to be able to answer fundamental questions such as "Is my security better this year?," "What am I getting for my security dollars?," or "How do I compare with my peers?").

[236] For a brief discussion of the importance of such information see ADAM SHOSTACK, AVOIDING LIABILITY: AN ALTERNATIVE ROUTE TO MORE SECURE PRODUCTS 3 (Fourth WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, WORKING PAPER, 2005), *available at* http://infosecon.net/workshop/pdf/44.pdf. *See also* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 30 et seq. (2007) (emphasizing the importance of *objective* data when it comes to software security).

[237] Microsoft has developed and publicly documented its software development process, the Security Development Lifecycle (SDL). *See* MICHAEL HOWARD & STEVE LIPNER, THE SECURITY DEVELOPMENT LIFECYCLE: SDL: A PROCESS FOR DEVELOPING DEMONSTRABLY MORE SECURE SOFTWARE 27 et seq. (2006) (discussing the history of SDL at Microsoft). *See* MICROSOFT CORP., MICROSOFT SECURITY DEVELOPMENT LIFECYCLE (SDL) – VERSION 5.0 (2010), *available at* http://www.microsoft.com/downloads/details.aspx?FamilyID=7d8e6144-8276-4a62-a4c8-7af77c06b7ac&displaylang=en.

[238] *Cf. infra* chapter 6.3 (discussing legal obligations to notify network security breaches).

[239] One of the few online service providers that do disclose this type of information is Google with regard to its Apps services. *See* http://www.google.com/appsstatus (last accessed Feb. 10, 2011).

[240] For a discussion of mandatory data security breach notification see *infra* chapter 6.2.

The second issue regards the perceived difficulty of measuring security.[241] It has to be pointed out that some of the perceived difficulties are rooted in misconceptions about different aspects of measurement. First, measurement is often understood as the elimination of uncertainty (which is almost never possible) instead of the *reduction of uncertainty*.[242] Second, the object of measurement—in our case "information security"—is often not clearly understood which of course renders its measurement impossible.[243] Third, people are often not aware of the available methods of measurement (such as various sampling procedures or types of controlled experiments).[244]

For example, information about publicly disclosed vulnerabilities could be used to measure the security of standard software (whether open source or proprietary).[245] However, in practice such measurements are rarely performed by customers, consultants, or trade magazines.

In recent years, security measurement research and standardization efforts have made significant progress, in particular with regard to measuring information security within an organization.[246] However, adoption is not widespread and many of those organizations that do

[241] *Cf., e.g.,* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 188 (2010) (stating that "many in the IT security industry seem to have a deeply rooted disposition against the very idea that security is measurable at all").

[242] *Cf. id.* at 23.

[243] *Cf. id.* at 27. *Cf. also* DEBRA S. HERRMANN, COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS: MEASURING REGULATORY COMPLIANCE, OPERATIONAL RESILIENCE, AND ROI 9 (2007) (noting that "[t]he problem is that many people […] have a vague, distorted, incomplete, fragmented, or microscopic understanding of IT security").

[244] *Cf.* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 28 (2010).

[245] *See infra* chapter 9.2.4 (proposing the introduction of a mandatory common software security metric).

[246] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT – MEASUREMENT, ISO/IEC 27004:2009 (2009) (providing guidance on the measurement of the

perform measurements rather focus on what they perceive as easy to measure on an operational level (e.g. the number of viruses detected each month) instead of attempting to actually reduce uncertainty for decision makers.[247]

Both facts taken together—that only little security-related information about products and services is publicly available and that the practice of measuring security based on that information is not widespread—generally result in uninformed and therefore rather poor risk decisions.

The direct consequence of these uninformed risk decisions is more risk exposure for information assets than otherwise achievable. However, there is also an important indirect consequence: since the customers' decisions do not, to a significant extent, take the security properties of products and services into account, software manufacturers and service providers have few incentives to invest in the security of their products and services.

In economics, situations like these, where one party to a transaction has more or better information than the other, are described as an instance of information asymmetry that may lead to a "market of lemons."[248] In such a market, only the low quality products ("lemons") are being sold: at first, buyers—who do not have the information to distinguish high from low

effectiveness of an implemented information security management system as defined in ISO/IEC 27001); NIST, PERFORMANCE MEASUREMENT GUIDE FOR INFORMATION SECURITY, SPECIAL PUBLICATION 800-55 REV. 1 (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf (providing guidance on the measurement of the effectiveness of security controls applied to information systems and supporting information security programs). Recent publications include ANDREW JAQUITH, SECURITY METRICS: REPLACING FEAR, UNCERTAINTY, AND DOUBT (2007); DEBRA S. HERRMANN, COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS: MEASURING REGULATORY COMPLIANCE, OPERATIONAL RESILIENCE, AND ROI (2007); and W. KRAG BROTBY, INFORMATION SECURITY MANAGEMENT METRICS: A DEFINITIVE GUIDE TO EFFECTIVE SECURITY MONITORING AND MEASUREMENT (2009).

[247] *Id.* at 78 (stating that most current security metrics are not very effective).

[248] *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. OF ECON. 488 (1970).

quality products—may be willing to buy for the average of the market value of a high and a low quality product if they estimate that the probability of getting either one is 50%. Sellers, however, who do have the information to distinguish high from low quality products, will only sell their low quality products because the average price offered by the buyers would be below the market value of the high quality products. Once buyers observe this, they will only be willing to pay the market value of a low quality product. This means that in situations where sellers have more information than buyers, there will be severe downward pressure on both price and quality.

The markets for software, Internet access services, and online services all exhibit these characteristics as far as information security is concerned.[249]

2.4.4. The Misalignment Between Risk and Risk Mitigation Capability

Currently, the entities most capable of mitigating many information security risks, do not suffer any damages should the risk materialize. The entities on the other hand, that do suffer damages, often do not have the capability to perform any risk mitigation. This can be described as a misalignment between risk and risk mitigation capability.[250]

[249] *See* Ross Anderson, *Why Information Security is Hard – An Economic Perspective*, 17 ANN. COMPUTER SECURITY APPLICATIONS CONF. 358, 362 (2001); ROSS ANDERSON ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET 18 (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport; Bruce Schneier, *How Security Companies Sucker Us With Lemons*, WIRED, Apr. 19, 2007, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2007/04/securitymatters_0419 *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 163 (2008). *Cf.* Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior, in* ECONOMICS OF INFORMATION SECURITY 165, 171 (L. Jean Camp & Stephen Lewis eds., 2004) (discussing the market of lemons in the context of the decision process of individuals with respect to their privacy and information security concerns). *Cf. also* ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 89 (2008); DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 64 (2008) (discussing the software market); Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 314 (2006) (discussing the software market).

[250] *Cf.* BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 270 (2006) (noting the importance of "align[ing] the security interests of players with their capabilities"); Bruce

For example, software manufacturers typically do not bear any of the risks associated with security vulnerabilities in their products unless they have to face liability for the low level of information security provided by their products.[251] Software manufacturers do not have to fear a drop in their market share because—as described *supra*—the relative security of software products is generally not transparent to customers.[252] Accordingly, in the absence of liability, software vulnerabilities do not constitute a significant risk for software manufacturers. The manufacturer's customers, however, bear the majority of the risks associated with software vulnerabilities but typically have no capabilities to mitigate those risks.[253]

Similarly, online service providers (and businesses in general) are typically the only ones who can strengthen the confidentiality, integrity, and availability of the data they store on behalf of their customers. However, absent regulatory intervention,[254] the market of online services is not sufficiently transparent with regard to information security to enable customers to

Schneier, *Make Vendors Liable for Bugs*, WIRED, June 6, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/06/71032, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 147, 147 (2008) (noting that there is "a very important rule about security: It works best when you align interests with capability").

[251] *Cf.* Bruce Schneier, *Make Vendors Liable for Bugs*, WIRED, June 6, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/06/71032, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 147, 148 (2008) (arguing for the introduction of software liability because "[s]oftware vendors are in the best position to improve software security" but "don't have much interest [in doing so]"); SCIENCE AND TECHNOLOGY COMMITTEE, PERSONAL INTERNET SECURITY VOLUME I: REPORT, 2006-7, H.L. 165–I, at 41-42, *available at* http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf (stating that software manufacturers "are all too easily able to dump risks onto consumers through licensing agreements, so avoiding paying the costs of insecurity"). *Cf. also infra* chapter 5.3 (discussing the liability of software manufacturers).

[252] *See supra* chapter 2.4.3.

[253] *Cf.* SCIENCE AND TECHNOLOGY COMMITTEE, PERSONAL INTERNET SECURITY VOLUME I: REPORT, 2006-7, H.L. 165–I, at 81, *available at* http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf (noting that "[t]he current assumption that end-users should be responsible for security is inefficient and unrealistic").

[254] *See infra* chapter 6.2 (discussing data security breach notification).

"punish" providers for comparatively low security. If there is no such transparency and if online service providers are not held liable for security breaches,[255] they hardly bear any of the risks resulting from the low level of security of their services.

Internet access providers are similarly situated—in particular with regard to the degree of network availability they are able to provide to their customers. While they are the only ones able to mitigate the risks of lost availability, they usually disclaim liability by contractual means and also refuse to disclose information about previous outages.[256]

In the literature on economics of information security, this misalignment between risk and risk mitigation capability is often described in terms of externalities.[257] Externalities are instances where an entity's actions have (positive or negative) economic consequences for third parties for which there is no compensation.[258] For example, a company that increases the security of its systems might create a positive externality for its business partners because they benefit from the fact that the risk that an attacker might use the company's network to attack them has been reduced. However, due to the lack of compensation, positive

[255] *See supra* chapter 5.1 (discussing the issue of liability for security breaches).

[256] *See supra* chapter 6.3 (discussing network security breach notification).

[257] *See* Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610, 610 (2006); L. Jean Camp, *The State of Economics of Information Security*, 2 I/S: J.L. & POL'Y 189, 194 (2006); ROSS ANDERSON ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET 18 (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport; L. Jean Camp & Catherine Wolfram, *Pricing Security: A Market In Vulnerabilities, in* ECONOMICS OF INFORMATION SECURITY 17, 18 (L. Jean Camp & Stephen Lewis eds., 2004); Bruce K. Kobayashi, *Private versus Social Incentives in Cybersecurity: Law and Economics, in* THE LAW AND ECONOMICS OF CYBERSECURITY 13, 16 (Mark F. Grady & Francesco Parisi eds., 2006); Bruce Schneier, *Information Security and Externalities*, ENISA Q. REV. (ENISA, Heraklion, Greece), Jan. 2007, at 3, *available at* http://www.enisa.europa.eu/publications/eqr/issues/eqr-q4-2006-vol.-2-no.-4/at_download/issue; Marc Lelarge & Jean Bolot, *Network Externalities and the Deployment of Security Features and Protocols in the Internet*, 2008 ACM SIGMETRICS 37.

[258] *Cf. generally* HAL R. VARIAN, INTERMEDIATE MICROECONOMICS: A MODERN APPROACH 626 et seq. (7th ed. 2005). *Cf. also* Charles T. Clotfelter, *Private security and the public safety*, 5 J. OF URB. ECON. 388 (1978) (discussing externalities in the context of public safety).

externalities are under-provided while negative externalities are over-provided. For example, a software manufacturer that decides to invest less in the security of his products creates a negative externality with regard to his customers.[259]

[259] *Cf.* L. Jean Camp & Catherine Wolfram, *Pricing Security: A Market In Vulnerabilities, in* ECONOMICS OF INFORMATION SECURITY 17, 20 (L. Jean Camp & Stephen Lewis eds., 2004) (noting that "[b]ecause security is an externality, software and hardware prices do not reflect the possibility of and the extent of the damages from associated security failures").

3. A Methodology for Assessing Regulatory Policies

To assess regulatory policies in any meaningful way, an assessment methodology is needed. The methodology developed below is centered on the concept of information security risk and the different regulatory options for treating that risk.

3.1. Information Security Risk Defined

Information security risk is often defined very generally as the "combination of the probability of an event and its consequence."[260] In that case, it is assessed in qualitative or quantitative terms.[261] In the latter case, it is typically measured in terms of an Annualized Loss Expectancy (ALE) which is defined follows[262]:

*ALE = Annualized Rate of Occurrence (ARO) * Single Loss Expectancy (SLE)*

ARO is used to express the probability of an event in terms of how often it occurs per year while SLE is used to express the consequences of that event. However, such a formula is rather impractical for the purpose of policy assessment as it does not provide an insight into the way in which a given regulatory policy might affect the risk. Furthermore, obtaining sufficient evidence to estimate how a given policy might affect the ARO or the SLE is

[260] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.34 (2009).

[261] For a comparison of quantitative and qualitative methods see, for example, THOMAS R. PELTIER, INFORMATION SECURITY RISK ANALYSIS 77 (2d ed. 2005); Kevin Henry, *Risk Management and Analysis, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 321, 322, 324 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007). *See also infra* chapter 4.1.10.4 for a discussion of the advantages and disadvantages of both methods when determining which safeguards are to be considered "reasonable" or "appropriate" under various laws and regulations.

[262] *See, e.g.,* DOUGLAS J. LANDOLL, THE SECURITY RISK ASSESSMENT HANDBOOK 416 (2006); Carl F. Endorf, *Measuring ROI on Security, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 133, 135 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007).

currently nearly impossible.[263] In practice, ALE, while mathematically precise, has proven to be ultimately a very subjective measurement. Contrary to the objectivity suggested by the mathematical simplicity, ALE often leads to highly subjective results as it is very difficult to establish—in an objective and repeatable way—the rate of occurrence (ARO) or the value of an information asset (and subsequently the SLE).[264]

To provide a clearer view on how regulatory policies affect risk, this thesis uses a definition that concentrates on the logical components of risks, attempting to model rather than measure information security risks. This definition is based on but significantly extends definitions previously presented in the literature.[265]

For the purpose of this thesis, "information security risk" is defined as the probability that a *threat agent* will give rise to a *threat* that exploits a *vulnerability* of an *information asset*, circumvents potential *safeguards* and thereby causes harm to an organization or an individual.

[263] *See* chapter 2.4.3 (discussing the difficulty of measuring security).

[264] *See* ANDREW JAQUITH, SECURITY METRICS: REPLACING FEAR, UNCERTAINTY, AND DOUBT 31 (2007); GERMAN BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK [BSI], RISK ANALYSIS BASED ON IT-GRUNDSCHUTZ, BSI-STANDARD 100-3, VERSION 2.5, at 5 (2008), *available at* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile (stating that "it has been proven that assessing the probability is often difficult in practice because there is no basis for reliable estimates" and that "[t]he interpretation of the probabilities is also frequently questionable").

[265] A definition that—beyond taking into account probability and impact—also considers the risk components of a threat and a vulnerability can be found in INFORMATION SECURITY MANAGEMENT HANDBOOK 3121 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) and OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 969 (Harold F. Tipton ed., 2007). A definition that refers to a threat, a vulnerability, and an asset can be found in ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY RISK MANAGEMENT, ISO/IEC 27005:2008 § 3.2 (2008) and ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – MANAGEMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY – PART 1: CONCEPTS AND MODELS FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY MANAGEMENT, ISO/IEC 13335-1:2004 § 2.19 (2004). A definition that refers to a vulnerability and a threat agent (but not a threat) can be found in SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 54 (5th ed. 2010). Note, however, that the risk components of a threat agent, a threat, a vulnerability, a safeguard, and an asset are nevertheless discussed in most of the sources cited above. Models that show how these components relate to the concept of risk can be found in: SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 55 (5th ed. 2010) (adding a "exposure" component) and ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – EVALUATION CRITERIA FOR IT SECURITY – PART 1: INTRODUCTION AND GENERAL MODEL, ISO/IEC 15408-1:2009 § 6.2 (2009) (not including a "vulnerability" component).

Note that this definition does contain the elements of probability and harm which are equivalent to the ARO and the SLE. However, these are only to be understood as the result of the interaction of the different risk components which are of primary importance. To which extent the risk components influence probability and harm cannot be calculated in a sufficiently objective way. While the definition of information security risk recognizes the importance of probability and harm, the methodology does not concern itself with these two measures but only with the risk components that will ultimately determine them.

The five risk components are (1) information asset, (2) vulnerability, (3) safeguard, (4) threat, and (5) threat agent. They are defined as follows:

An *information asset* is "knowledge or data that has value to the organization."[266] Very often, information is maintained in an electronic form in which case it is also referred to as "data." However, it has to be emphasized that the term "information asset" also covers non-electronic information.

The different security properties of a single information asset can be of value to different entities. For example, let's consider a marketing company's database storing the names and addresses of individuals along with their marital statuses and levels of income. The availability of this information asset is only of value to the marketing company but not the individuals concerned. The asset's confidentiality, on the other hand, is only of value to the individuals concerned but not to the marketing company.[267]

[266] ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.18 (2009).

[267] Assuming, of course, that the company did not derive a competitive advantage from the asset's confidentiality. Note that a particularly challenging question with regard to information assets is how to measure their value. This issue is further explored *supra* in chapter 4.1.10.4.

A *vulnerability* is defined as a weakness of an information asset or safeguard that can be exploited by a threat.[268] Vulnerabilities can either be of a technical, administrative, or physical nature.[269]

Technical vulnerabilities are implemented in computer hard- and, in particular, software. As regards software vulnerabilities, the Common Vulnerabilities and Exposures (CVE) Initiative maintained by the MITRE Corporation[270] provides identifiers for publicly known vulnerabilities. When a specific vulnerability is referenced in this thesis, it will be referred to by its CVE Identifier (e.g. CVE-2010-1885) for which detailed information will be available via the National Vulnerability Database.[271] In an effort to reach consensus among the various stakeholder (including software manufacturers), the CVE Initiative defines a software vulnerability rather narrowly as "a mistake in software that can be directly used by a hacker to gain access to a system or network."[272] Additionally, it introduced the term "exposure" which refers to "a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network."[273] For the purpose of this thesis, software vulnerabilities and exposures as defined by the CVE Initiative are collectively referred as "software vulnerabilities." The most

[268] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.46 (2009) (defining "vulnerability" as "weakness of an asset or control that can be exploited by a threat").

[269] *Cf.* DOUGLAS J. LANDOLL, THE SECURITY RISK ASSESSMENT HANDBOOK 35 (2006).

[270] The CVE Initiative is sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security. *See* http://cve.mitre.org (last accessed Feb. 10, 2011).

[271] *See* http://nvd.nist.gov (last accessed Feb. 10, 2011). Details for a particular CVE Identifier can be obtained via the NVD's search feature or, more directly, by requesting a URL in a web browser that consists of the string "http://nvd.nist.gov/nvd.cfm?cvename=" followed by the CVE Identifier, e.g., http://nvd.nist.gov/nvd.cfm?cvename=CVE-2010-1885.

[272] *See* http://cve.mitre.org/about/terminology.html (last accessed Feb. 10, 2011).

[273] *See id.*

dangerous[274] types of software vulnerabilities include buffer overflows,[275] SQL injection vulnerabilities,[276] and cross-site scripting (XSS) vulnerabilities.[277]

These software vulnerabilities are introduced during the software development process.[278] However, it is important to recognize that vulnerabilities may not only be created by software manufacturers but also by individuals and organizations using the software.[279] Most vulnerabilities that fall into this category are created by insecure software configuration

[274] The SANS Institute and MITRE Corporation's Common Weakness Enumeration (CWE) Initiative publish a list of the most dangerous types of vulnerabilities on a yearly basis: "CWE/SANS Top 25 Most Dangerous Software Errors." *See* http://cwe.mitre.org/top25/index.html#Listing (last accessed Feb. 10, 2011).

[275] A buffer overflow occurs when a program writes more data to a buffer than the buffer can hold, thereby overwriting adjacent memory. If an attacker can directly influence the exact data that is written over the adjacent memory, he can overwrite the memory with his own program code. The MITRE Corporation's Common Weakness Enumeration (CWE) Initiative refers to this type of vulnerability as CWE-120 ("Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')"). *See* http://cwe.mitre.org/data/definitions/120.html (last accessed Feb. 10, 2011). *Cf. also* Aleph1, *Smashing The Stack For Fun And Profit*, PHRACK, Nov. 8, 1996, http://www.phrack.org/issues.html?issue=49&id=14#article (providing the first in-depth description of how to exploit stack-based buffer overflows). For an extensive discussion of stack-based and heap-based buffer overflows see JAMES C. FOSTER ET AL., BUFFER OVERFLOW ATTACKS: DETECT, EXPLOIT, PREVENT 161, 229 (2005).

[276] Web applications can be viewed as consisting of three tiers: the client tier (i.e. a web browser), the middle tier (i.e. a web server that allows application-specific logic to be implemented), and the data tier (typically a relational database server). If the data tier is indeed a relational database, the Structured Query Language (SQL) is used for the communication between the middle tier and the data tier. If the middle tier constructs part of an SQL command using input provided from the client tier and does not correctly neutralize that input, an attacker can inject his own SQL statements which might allow him to delete, modify, or obtain data that is stored in the database. The CWE Initiative refers to this type of vulnerability as CWE-89 ("Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')"). *See* http://cwe.mitre.org/data/definitions/89.html (last accessed Feb. 10, 2011). *Cf. generally* JUSTIN CLARKE, SQL INJECTION ATTACKS AND DEFENSE (2009).

[277] XSS is possible if a website does not correctly neutralize user-controllable input (e.g. the text entered as a new entry in an online discussion forum) before using it in output that is sent to other users' browsers (e.g. a discussion thread that also displays the attacker's message). This enables an attacker to place script code on a web page that will be executed by every user's browser upon visiting that web page. The CWE Initiative refers to this type of vulnerability as CWE-79 ("Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')"). *See* http://cwe.mitre.org/data/definitions/79.html (last accessed Feb. 10, 2011). *Cf. also* DAFYDD STUTTARD & MARCUS PINTO, THE WEB APPLICATION HACKER'S HANDBOOK: DISCOVERING AND EXPLOITING SECURITY FLAWS 376 et seq. (2008).

[278] Typically, these three types of vulnerabilities are introduced at the implementation stage of software development. *Cf.* MARK G. GRAFF & KENNETH R. VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES 30, 55, 99, 124 (2003) (differentiating between vulnerabilities that are introduced at the architecture, design, implementation, or operations stage of software development).

[279] *Id.* at 124 (discussing the challenges of a reasonable secure software operations environment).

settings (e.g. setting the wrong file permissions on a network resource or enabling cryptographic algorithms that are easy to break) or choosing weak authenticators (e.g. a password that can be easily guessed).

Vulnerabilities that are not of a technical but of an administrative nature concern weaknesses in an organization's policies, procedures, or guidelines. Examples include insufficient (or lacking) employee termination procedures that would ensure that an employee's system account is immediately locked or removed upon termination,[280] insufficient change-of-employment procedures that would prevent the unnecessary accumulation of system privileges (also referred to as authorization creep),[281] or insufficient procedures that would prevent the sharing of system accounts thereby eliminating accountability (e.g. all users of a system using a single administrative account).

Physical vulnerabilities include unguarded entrances, unlocked doors or easily picked locks. Despite being much more of a common day nature, physical vulnerabilities are often overlooked by professionals that have a background in technology or management.

Safeguards (synonymous with security controls or countermeasures) are the third risk component and refer to any means of mitigating a risk. Like vulnerabilities, safeguards can be either technical (e.g. a firewall or a network intrusion detection system), administrative (e.g. company policies, procedures, and guidelines), or physical (e.g. armed guards or a video

[280] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, ISO/IEC 27002:2005 § 8.3 (2005) (discussing safeguards in the context of termination or change of employment).

[281] *Cf.* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 197 (5th ed. 2010).

surveillance system).[282] The nature of a safeguard can be deterrent, preventive, detective, or reactive.[283] *Deterrent controls* are designed to deter malicious threat agents (e.g. an employee sanction policy) while *preventive controls* are intended to avoid the occurrence of unwanted events (e.g. a firewall preventing certain network attacks) and *detective controls* attempt to identify unwanted events after they have occurred (e.g. intrusion detection systems). Lastly, *reactive controls* (sometimes also referred to as corrective and/or recovery controls)[284] are typically triggered by detective controls and are designed to remedy the situation identified by a detective control, usually by reducing the impact of a threat that has already materialized (e.g. a disaster recovery plan or a backup system that allows for a quick restore after an incident).

A *threat* is defined as the cause of a potential unwanted incident that may result in the exploitation of a vulnerability and, subsequently, in harm to an information asset.[285] Examples

[282] *See* Harold F. Tipton, *Types of Information Security Controls, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1357 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007). The security requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPPA) are also classified in this way. *See infra* chapter 4.1.1. For an alternative classification scheme see NIST, RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, SPECIAL PUBLICATION 800-53 REV. 3, at 6 (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf (differentiating between management, operational, and technical security controls).

[283] *See* Harold F. Tipton, *Types of Information Security Controls, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1357 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007). *Cf. also* Sean M. Price, *Operations Security, in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 633, 646 (Harold F. Tipton ed., 2007); JAMES E. PURCELL, SECURITY CONTROL TYPES AND OPERATIONAL SECURITY (2007), http://www.giac.org/resources/whitepaper/operations/207.pdf.

[284] The information security profession usually does not use the term reactive control but rather distinguishes between corrective controls and recovery controls. *Cf.* Harold F. Tipton, *Types of Information Security Controls, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1357 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007). However, since this distinction is not very precise, this thesis will only use the more general term "reactive control."

[285] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.45 (2009) (defining "threat" as "potential cause of an unwanted incident, which may result in harm to a system or organization").

are theft,[286] dumpster diving,[287] social engineering,[288] denial of service attacks,[289] phishing,[290] and malicious software (referred to as *malware*). The particular importance of the last category warrants further explanation.

Malware can be categorized by the way it is installed on a system: First, users can be made to voluntarily execute a program that appears benign but actually has a hidden malicious purpose in which case the malware is referred to as a Trojan horse.[291] Second, malware can be installed by making a user visit a web page or open an e-mail message that contains code that exploits a vulnerability of the web browser, e-mail client, or operating system which secretly installs the malware (without requiring any further user interaction).[292] Such malware is referred to as a drive-by download. Third, malware can self-replicate in an automated fashion

[286] The theft of laptops has been a particular concern. *Cf.* PONEMON INST., BUSINESS RISK OF A LOST LAPTOP: A STUDY OF IT PRACTITIONERS IN THE UNITED STATES, UNITED KINGDOM, GERMANY, FRANCE, MEXICO & BRAZIL (2009), *available at* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/The%20Business%20Risk%20of%20a%20Lost%20Laptop%20%28Global%29%20Final%204.pdf.

[287] This describes the practice of searching through the victim's trash in an attempt to obtain valuable information. For an extensive discussion see JOHNNY LONG, NO TECH HACKING: A GUIDE TO SOCIAL ENGINEERING, DUMPSTER DIVING, AND SHOULDER SURFING 1 et seq. (2008).

[288] This describes the practice of manipulating people in an attempt to make them disclose confidential information or perform other actions that compromise information. *See supra* chapter 2.4.2.

[289] Denial of service attacks compromise the availability of information either by destroying the system that makes the information available, exhausting the system's resources, or causing the service to crash. *Cf.* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 767 et seq. (3d ed. 2003).

[290] Phishing is a specific form of social engineering. It can be defined as "[t]he act of sending to a user an e-mail falsely claiming to be an established legitimate enterprise in an attempt to trick the user into surrendering personal or private information." *See* Stephen D. Fried, *Phishing: A New Twist to an Old Game, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 2853 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007).

[291] *See* NIST, GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING, SPECIAL PUBLICATION 800-83, at 2-4 (2005), *available at* http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf. This type of malware is named after the wooden horse from Greek mythology. Unfortunately, the term Trojan—which, if we continued the analogy, would refer to the victim of a Trojan horse attack—is often used synonymous with Trojan horse.

[292] *Cf., e.g.,* Manuel Egele et al., *Mitigating Drive-By Download Attacks: Challenges and Open Problems, in* INETSEC 2009 – OPEN RESEARCH PROBLEMS IN NETWORK SECURITY 52 (Jan Camenisch & Dogan Kesdogan eds., 2009).

and execute itself without user intervention in which case it is referred to as a worm.[293] Forth, if it is self-replicating but requires user interaction to execute (e.g. a user opening an infected PDF file) it is called a virus.[294]

Once installed on a system, malware may provide various "features" to the attacker. It may spy on the user in an attempt to obtain valuable information such as credit card data. Such malware is referred to as spyware. If it displays unsolicited advertisements, it is referred to as adware. Malware that generally provides the attacker with full remote control over a compromised system (including peripheral devices such as a webcam or a microphone) is referred to as a remote administration tool (RAT).[295] If the malware modifies the operating system to ensure that it—or other malware—retains the privileges of the administrative account ("root" under UNIX and Linux) without being detectable, it is referred to as a "rootkit."[296]

The fifth risk component, the *threat agent*, refers to the entity that causes a threat to happen.[297] A threat agent can be either a human (e.g. an employee, a contractor, or an

[293] *See* NIST, GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING, SPECIAL PUBLICATION 800-83, at 2-3 (2005), *available at* http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.

[294] *See id.* at 2-1; SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 742 (3d ed. 2003).

[295] *See* NIST, GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING, SPECIAL PUBLICATION 800-83, at 2-7 (2005), *available at* http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf. Unfortunately, the nonsensical term Remote Access Trojan is sometimes also used. *See, e.g.,* CRAIG A. SCHILLER ET AL., BOTNETS: THE KILLER WEB APP 33 (2007).

[296] *See* GREG HOGLUND & JAMIE BUTLER, ROOTKITS: SUBVERTING THE WINDOWS KERNEL 2 (2005) (stating that "[a] rootkit is a 'kit' consisting of small and useful programs that allow an attacker to maintain access to 'root,' the most powerful user on a computer" and further stating that "[i]n other words, a rootkit is a set of programs and code that allows a permanent or consistent, undetectable presence on a computer").

[297] *See* DOUGLAS J. LANDOLL, THE SECURITY RISK ASSESSMENT HANDBOOK 31 (2006). *Cf.* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 54 (5th ed. 2010) (defining "threat agent" as "[t]he entity that takes advantage of a vulnerability"); NIST, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 200, at 9 (2006), *available at* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (stating that "threat agent" is

outsider) or nature (e.g. a storm, a flood, or rodents).[298] It should be pointed out that human threat agents do not necessarily act out of malicious intent (as discussed *supra* in chapter 2.3.7) but might also make errors or mistakes, whether negligently or not.

3.2. Risk Treatment Options

Any regulatory policy that addresses information security risks can do so in a number of ways: it can aim to mitigate, avoid, transfer, or retain risks. These options are collectively referred to as risk treatment options.[299]

3.2.1. Risk Mitigation

The regulatory option of risk mitigation (also referred to as risk reduction) describes the process of reducing a risk by implementing (or mandating the implementation of) safeguards.[300] In particular, these safeguards can mitigate risks by reducing information assets,[301] reducing vulnerabilities, reducing the number, motivation, or capabilities of threat agents, or by generally making it more difficult for threat agents to mount a threat. Measures of risk mitigation can also be classified as deterrent, preventive, detective, or reactive.[302]

synonymous with "threat source" and defining it as "[t]he intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability").

[298] *Cf.* DOUGLAS J. LANDOLL, THE SECURITY RISK ASSESSMENT HANDBOOK 31 (2006).

[299] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY RISK MANAGEMENT, ISO/IEC 27005:2008 § 9.1 (2008) (stating that there are four options available for risk treatment: risk reduction, risk retention, risk avoidance, and risk transfer). *Cf. also* DOUGLAS J. LANDOLL, THE SECURITY RISK ASSESSMENT HANDBOOK 39 (2006) (using the term "risk resolution" instead of "risk treatment" and defining as "the decision by senior management of how to resolve the risk [presented] to them").

[300] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY RISK MANAGEMENT, ISO/IEC 27005:2008 § 3.7 (2008) (defining risk reduction as "actions taken to lessen the probability, negative consequences, or both, associated with a risk").

[301] By reducing the quantity or quality of assets, the potential harm that can be caused by compromising the assets is typically reduced as well.

[302] *Cf. supra* chapter 3.1.

From a regulator's or legislator's perspective, risk mitigation can be achieved in one of two ways: in a direct or an indirect (mandated) fashion.

3.2.1.1. Direct Risk Mitigation

The term direct risk mitigation is used here to refer to regulatory or legislative actions that reduce risks directly, without the need for any further action by an entity other than the regulator or legislator.

Since regulatory and legislative bodies store, process, or transmit only very few information assets themselves, the scope of possible direct risk mitigation measures is rather narrow. For example, no regulatory action can directly improve the effectiveness of technical safeguards implemented by online service providers or can directly reduce the number of vulnerabilities in standard software. However, there is one particular area in which private actors can do very little while regulators and legislators can directly mitigate risks rather effectively: the deterrence of malicious threat agents. Civil and in particular criminal liability can be an important instrument to deter malicious threat agents from carrying out any attacks. Obviously, risks caused by accidents or natural forces are not addressed by deterrent measures.

However, it has to be recognized that deterrence, while important, only mitigates those risks that are caused by malicious threat agents but does not address risks caused by accidents or natural disasters.

3.2.1.2. Indirect Risk Mitigation

A legislator or regulator can indirectly mitigate risks by mandating that regulated entities implement security controls. This mandate can be rather vague (e.g. requiring "adequate," "reasonable," or "appropriate" security controls) or very specific (e.g. requiring that information be encrypted or that certain information destruction processes be implemented).

With regard to detective security controls (controls that attempt to identify unwanted events after they have occurred), it is important to note that by themselves they actually do not reduce any risks. Their value lies in the fact that they enable those who are notified about the unwanted events to (1) take reactive security measures to reduce the impact of a threat that has already materialized and (2) make more informed risk decisions in the future. Different detective controls may require the notification of different entities such as the regulated entity itself (or its senior management), the regulator (or legislator), or other third parties that have an interest in the information assets.

3.2.2. Risk Avoidance

This risk treatment option aims at the discontinuation of the activity that is causing the risk.[303] Like risk mitigation, it can be of direct or indirect (i.e. mandated) nature.

Indirect risk avoidance may be implemented by mandating that a vulnerability be eliminated (e.g. mandating that public key authentication be used instead of password authentication in order to eliminate the vulnerability of weak passwords).[304] To not only avoid the risk associated with a particular vulnerability but to eliminate all risks to which a particular information asset is exposed, a regulator or legislator may mandate the elimination of the asset itself (e.g. prohibiting the retention of certain data, thereby eliminating the risk that the retained data may be compromised). The elimination of information assets may be worth of consideration in particular in situations where the information security risk of the loss of

[303] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY RISK MANAGEMENT, ISO/IEC 27005:2008 § 3.3 (2008) (defining risk avoidance as the "decision not to become involved in, or action to withdraw from, a risk situation").

[304] *Cf., e.g.,* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 76, 90 (3d ed. 2003) (discussing the vulnerabilities associated with password authentication as well as the advantages and disadvantages of public key authentication).

confidentiality and/or integrity outweighs the benefits resulting from the information's availability.

3.2.3. Risk Transfer

This regulatory option aims at transferring risk from one entity to another.[305] It is particularly well suited to address one of the fundamental challenges of information security identified above: the misalignment between risk and risk mitigation capability. A regulator or legislator may chose to transfer risk directly or indirectly.

3.2.3.1. Direct Risk Transfer

The term direct risk transfer is used here to refer to regulatory or legislative actions that transfer risks from one entity to another directly, without the need for any further action by an entity other than the regulator or legislator.

The most straightforward means of direct risk transfer is the introduction of civil liability. By making one entity liable for the damages suffered by another entity in the case that a particular risk materializes, that risk is directly transferred to the liable entity.

To implement a partial direct risk transfer, liability may be assigned for only a portion of the damages. Furthermore, statutory warranties may partially transfer risks associated with certain products or services to the manufacturer or service provider by giving the customer the right to have the product brought into conformity free of charge, to have the price reduced appropriately, or to have the contract rescinded.

[305] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY RISK MANAGEMENT, ISO/IEC 27005:2008 § 3.9 (2008) (defining "risk transfer" as "sharing with another party the burden of loss […] for a risk")

3.2.3.2. Indirect Risk Transfer

A legislator or regulator can also indirectly transfer risk by mandating that certain entities take actions that result in a risk transfer. A very simple example would be a mandate to purchase insurance against security breaches. This would result in a risk transfer from the insurees to the insurer.

A type of indirect risk transfer of practical importance consists in mandatory disclosure of security-related information. As discussed above, one of the reasons manufacturers and service providers bear little of the risk that results from low levels of security of their products and services is that their market share is unlikely to drop due to the bad security of their products and services. This is because the relative security of products and services is generally not transparent to customers. However, if mandatory disclosure of security-related information allows customers to better judge the security of products and services, manufacturers and service provides would face the serious risk of financial losses due to a drop in their market share.

The mandatory disclosure of security-related information reduces the customers' risks by enabling them to make more informed risk decisions while,[306] at the same time, increasing the manufacturers' and service providers' risks by exposing them to competition with regard to the security properties of their products and services. Such a measure therefore effectively transfers risk from the customers to the manufacturers and service providers.[307]

[306] *Cf. supra* chapter 2.4.3 (discussing the fundamental challenge of uninformed risk decisions).

[307] Mandatory disclosure measures can therefore potentially perform risk transfers comparable to those created by liability regimes. *Cf., e.g.,* ADAM SHOSTACK, AVOIDING LIABILITY: AN ALTERNATIVE ROUTE TO MORE SECURE PRODUCTS (Fourth WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, WORKING PAPER, 2005), *available at* http://infosecon.net/workshop/pdf/44.pdf (arguing that to impose transparency rather than liability on software manufacturers could yield similar results).

The mandatory disclosure of security-related information can be considered a *targeted transparency policy* as defined by Fung et al.[308] Such policies mandate disclosure to trigger a change in the behavior of those to whom the information is disclosed (users), a change which in turn should provide incentives for disclosing entities to change their behavior.[309] It has been demonstrated that for a targeted transparency policy to have any effect, the new information has to become "embedded" into users' decision-making processes.[310] This depends on (1) the value users perceive the new information to have for achieving their own goals (e.g. increasing the security for their own information),[311] (2) the information's compatibility with user's decision-making processes in particular with regard to the information's format and time and place of availability,[312] and (3) the extent to which the new information can be easily comprehended by users.[313] To be not only effective but successful, a targeted transparency policy has to affect the users' buying decisions in a way that furthers the policy objective.

[308] *See* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 6 (2007) (defining the characteristics of targeted transparency policies as follows: (1) mandated public disclosure (2) by private or public organizations (3) of standardized, comparable, and disaggregated information (4) regarding specific products or practices (5) to further a defined public purpose). *Cf. also* Cass R. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613, 613 (1999) (referring to the same concept as "regulation through disclosure").

[309] *See* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 73 (2007).

[310] *See id.* at 54.

[311] *See id.* at 55.

[312] *See id.* at 56.

[313] *See id.* at 59.

3.2.4. Risk Retention

Risk retention (also referred to as risk acceptance) is a risk treatment option that consists in consciously accepting a certain risk.[314] Since there is no such thing as complete security, a residual risk will necessarily remain and has to be accepted. Furthermore risk retention might be the appropriate policy option when the overall (social) costs of mitigating, avoiding, or transferring certain risks are too high.

[314] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY RISK MANAGEMENT, ISO/IEC 27005:2008 § 3.8 (2008) (defining risk retention as the "acceptance of the burden of loss […] from a particular risk").

4. Regulating Information Security by Mandating Security Controls

One of the most obvious regulatory approaches to information security is to make the implementation of security controls mandatory, thereby hoping to mitigate risks indirectly. As the analysis below will demonstrate, there are different ways to follow this general approach.

Chapter 4.1 discusses exclusively laws and regulations that address personal information controllers (i.e. entities that control the processing of personal information).[315] Subsequent chapters will deal with mandatory controls for publicly traded companies (chapter 4.2), for service providers (chapter 4.3), for government authorities (chapter 4.4), and for software manufacturers (chapter 4.5).

Due to their mostly sector-specific nature, U.S. laws and regulations are more numerous than their equivalents under EU law. In consideration of this fact, each of the following chapters will first discuss the legal situation in the U.S. before turning to the legal situation in the EU.

4.1. Mandatory Security Controls for Personal Information Controllers

The following laws and regulations mandate the implementation of security controls for personal information controllers: the Security Rule of the Health Insurance Portability and Accountability Act (chapter 4.1.1), the Safeguards Rules of the Gramm-Leach-Bliley Act (chapter 4.1.2), the Fair Credit Reporting Act (chapter 4.1.3), the Children's Online Privacy Protection Act (chapter 4.1.4), the Communications Act (chapter 4.1.5), the Federal Trade Commission Act (chapter 4.1.6), various California and New York state laws (chapter 4.1.7), the EUDPD (chapter 4.1.8), and the EU ePrivacy Directive (chapter 4.1.9).

[315] *See* chapter 2.2.1 (introducing the term personal information controller).

4.1.1. The Health Insurance Portability and Accountability Act Security Rule

The Health Insurance Portability and Accountability Act of 1996[316] (hereinafter *HIPAA*) provided the U.S. Department of Health and Human Services (hereinafter *HHS*) with the statutory authority to promulgate, *inter alia*, "[s]ecurity standards for health information."[317] The Security Rule[318] subsequently promulgated by the HHS became effective on April 20, 2005.[319] It requires covered entities to implement specific safeguards to protect the confidentiality, integrity, and availability of certain health information. The personal scope of application (i.e. the range of covered entities) is limited to health plans, health care clearinghouses, health care providers, and their business associates.[320] The material scope of application is limited to "protected health information" (defined as "individually identifiable health information")[321] that is in electronic form (hereinafter *ePHI*).[322]

[316] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[317] 42 U.S.C. § 1320d-2(d) (2010).

[318] Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (codified as amended at 45 C.F.R. pts. 160, 162, 164). Pursuant to HIPAA § 264(c), the HHS also promulgated the Privacy Rule which is only concerned with confidentiality of protected health information. The Privacy Rule does not provide any detailed safeguards requirements. *See* Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified as amended at 45 C.F.R. pts. 160, 164).

[319] An exception was made for small health plans for which the Security Rule became effective on Apr. 20, 2006. 45 C.F.R. § 164.318(a)(2) (2010).

[320] 45 C.F.R. § 164.104(a) (2010). § 13401 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009), that was enacted on February 17, 2009, made 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 as well as 42 U.S.C. §§ 1320d–5, 1320d–6 also applicable for business associates of covered entities. *Cf.* Cynthia M. Conner et al., *American Health Lawyers Association 2008-2009 Year in Review,* 3 J. HEALTH & LIFE SCI. L. 1, 40 et seq. (2009). This extension of the personal scope of application addresses one of the most criticized deficiencies of HIPAA. *Cf.* Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L. J. 617, 618 (2002); Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV 331, 344 (2007). *Cf. also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 208 (2004).

[321] *See* 45 C.F.R. § 160.103.

[322] *See* 45 C.F.R. § 164.302. Protected health information (PHI) in non-electronic form (e.g. on paper) therefore falls outside of the scope of the Security Rule. Under the Privacy Rule, such information nonetheless requires the

On a general level, the Security Rule requires covered entities (1) to ensure the confidentiality,[323] integrity,[324] and availability[325] of all ePHI the covered entity creates, receives, maintains, or transmits; (2) to protect "against any reasonably anticipated threats or hazards to the security or integrity of such information"; (3) to protect against "any reasonably anticipated uses or disclosures of such information" that are not permitted or required under the Privacy Rule;[326] and (4) to ensure that their workforce complies with the Security Rule.[327]

More specifically, the Security Rule provides "standards" and "implementation specifications," the latter giving details for how to fulfill the obligations outlined in the standards. Implementation specifications are either required (i.e. mandatory)[328] or "addressable." Addressable implementation specifications have to be implemented if they are "reasonable and appropriate."[329] If that is not the case, the reason for it has to be documented and an alternative measure has to be implemented, if that is reasonable and appropriate.[330]

implementation of "appropriate administrative, technical, and physical safeguards" to ensure the privacy (i.e. confidentiality) of PHI. 15 C.F.R. 164.530(c). The Privacy Rule does not provide any further guidance regarding the selection of safeguards. *Cf.* Françoise Gilbert, *HIPAA Privacy and Security*, *in* A GUIDE TO HIPAA SECURITY AND THE LAW 9, 12, 17 (Stephen S. Wu ed., 2007).

[323] Confidentiality is defined as "the property that data or information is not made available or disclosed to unauthorized persons or processes." 45 C.F.R. § 164.304.

[324] Integrity is defined as "the property that data or information have not been altered or destroyed in an unauthorized manner." 45 C.F.R. § 164.304.

[325] Availability is defined as "the property that data or information is accessible and useable upon demand by an authorized person." 45 C.F.R. § 164.304.

[326] Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified as amended at 45 C.F.R. pts. 160, 164).

[327] *See* 45 C.F.R. § 164.306(a).

[328] *See* 45 C.F.R. § 164.306(d)(2).

[329] 45 C.F.R. § 164.306(d)(3)(ii)(A)

[330] 45 C.F.R. § 164.306(d)(3)(ii)(B).

The standards and implementation specifications are categorized as administrative,[331] physical,[332] or technical[333] safeguards.[334]

The standards to be implemented with regard to administrative safeguards are: a security management process,[335] the assignment of security responsibility,[336] implementation of workforce security,[337] information access management,[338] security awareness and training,[339] security incident procedures,[340] establishment of a contingency plan,[341] the performance of evaluations,[342] and the imposition of security requirements on business associates.[343]

[331] Defined as "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." 45 C.F.R. § 164.304.

[332] Defined as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." 45 C.F.R. § 164.304.

[333] Defined as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." 45 C.F.R. § 164.304.

[334] The Security Rule also requires covered entities to implement reasonable and appropriate policies and procedures to comply with the standards and implementation specifications. 45 C.F.R. § 164.316(a). Furthermore, 45 C.F.R. § 164.316(b) establishes additional documentation requirements.

[335] 45 C.F.R. § 164.308(a)(1)(i). This entails the following mandatory implementation specifications: risk analysis, risk management, sanction policy, and information system activity review. *See* 45 C.F.R. § 164.308(a)(1)(ii)(A)-(D).

[336] 45 C.F.R. § 164.308(a)(2).

[337] 45 C.F.R. § 164.308(a)(3)(i). This entails the following addressable implementation specifications: authorization and/or supervision, workforce clearance procedures, and termination procedures. *See* 45 C.F.R. § 164.308(a)(3)(ii)(A)-(C).

[338] 45 C.F.R. § 164.308(a)(4)(i). This entails the following implementation specifications: isolating health care clearinghouse functions (required), access authorization (addressable), and access establishment and modification (addressable). *See* 45 C.F.R. § 164.308(a)(4)(ii)(A)-(C).

[339] 45 C.F.R. § 164.308(a)(5)(i). This entails the following addressable implementation specifications: security reminders, protection from malicious software, log-in monitoring, and password management. *See* 45 C.F.R. § 164.308(a)(5)(ii)(A)-(D).

[340] 45 C.F.R. § 164.308(a)(6)(i). This entails one required implementation specification: response and reporting. *See* 45 C.F.R. § 164.308(a)(6)(ii).

[341] 45 C.F.R. § 164.308(a)(7)(i). This entails the following implementation specifications: data backup plan (required), disaster recovery plan (required), emergency mode operation plan (required), testing and revision

The standards for physical safeguards are facility access controls,[344] workstation use,[345] workstation security,[346] and device and media controls.[347]

The standards for technical safeguards are access control,[348] audit controls,[349] data integrity,[350] person or entity authentication,[351] and transmission security.[352]

These standards and the corresponding implementation specifications establish a rather detailed,[353] set of regulatory requirements while maintaining "technological neutrality"[354] and flexibility.

procedures (addressable), and applications and data criticality analysis (addressable). *See* 45 C.F.R. § 164.308(a)(7)(ii)(A)-(E).

[342] 45 C.F.R. § 164.308(a)(8).

[343] 45 C.F.R. § 164.308(b)(1).

[344] 45 C.F.R. § 164.310(a)(1). This entails the following addressable implementation specifications: contingency operations, facility security plan, access control and validation procedures, maintenance records. *See* 45 C.F.R. § 164.310(a)(2)(i)-(iv).

[345] 45 C.F.R. § 164.310(b).

[346] 45 C.F.R. § 164.310(c).

[347] 45 C.F.R. § 164.310(d)(1). This entails the following implementation specifications: ePHI disposal (required), media re-use (required), accountability (addressable), and data backup and storage (addressable). *See* 45 C.F.R. § 164.310(a)(2)(i)-(iv).

[348] 45 C.F.R. § 164.312(a)(1). This entails the following implementation specification: unique user identification (required), emergency access procedure (required), automatic logoff (addressable), and encryption and decryption (addressable). *See* 45 C.F.R. § 164.312(a)(2)(i)-(iv).

[349] 45 C.F.R. § 164.312(b).

[350] 45 C.F.R. § 164.312(c)(1). This entails one addressable implementation specification: a mechanism to authenticate ePHI. *See* 45 C.F.R. § 164.312(c)(2).

[351] 45 C.F.R. § 164.312(d).

[352] 45 C.F.R. § 164.312(e)(1). This entails the following addressable implementation specifications: integrity controls, and encryption. *See* 45 C.F.R. § 164.312(e)(2)(i)-(ii).

[353] For a discussion on how the Security Rule's standards and implementation specifications relate to the best practice recommendations contained in ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, ISO/IEC 27002:2005 (2005) see SHELDON BORKIN, THE HIPAA FINAL SECURITY STANDARDS AND ISO/IEC 17799 (2003), http://www.sans.org/reading_room/whitepapers/standards/the_hipaa_final_security_standards_and_iso/iec_17799_1193. *Cf. also* NIST, AN INTRODUCTORY RESOURCE GUIDE FOR IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND

To fulfill its obligations und the Security Rule, a covered entity may use any security measures that allow it to "reasonably and appropriately" implement the standards and implementation specifications.[355] In deciding which security measures to use, a covered entity must take into account its size, complexity, capabilities, and technical infrastructure; the security measures' costs; and the "probability and criticality of potential risks" to ePHI.[356]

The Security Rule's enforcement mechanisms have been criticized in the past for lack of effectiveness.[357] 42 U.S.C. § 1320d–5 as enacted by HIPAA provided civil penalties of not more than $100 for each violation and of no more than $25,000 for all violations of an identical provision during a calendar year. Furthermore, the Final Enforcement Rule promulgated by the HHS in 2006[358] identified a complaint-driven process and voluntary compliance as the primary enforcement strategy.[359] A private cause of action was also not provided (see *infra* chapter 5.1.1).

ACCOUNTABILITY ACT (HIPAA) SECURITY RULE, SPECIAL PUBLICATION 800-66 REV. 1 (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

[354] *Cf.* Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8,334, 8,341 (Feb. 20, 2003). *Cf.* C. Stephen Redhead, *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations*, *in* THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA): OVERVIEW AND ANALYSES 69 (Susan Boriotti & Donna Dennis eds., 2004).

[355] 45 C.F.R. § 164.306(b)(1).

[356] *See* 45 C.F.R. § 164.306(b)(2).

[357] *Cf., e.g.,* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV 331, 354 (2007). *Cf.* HEALTHCARE INFO. AND MGMT. SYS. SOC'Y & PHOENIX HEALTH SYS., U.S. HEALTHCARE INDUSTRY HIPAA COMPLIANCE SURVEY RESULTS: SUMMER 2005 (2005), *available at* http://www.himss.org/content/files/Summer_Survey_2005_Final.pdf (stating that the two most reported "roadblocks" to HIPAA compliance were "no public relations or brand problems anticipated with non-compliance" and "no anticipated legal consequences for non-compliance").

[358] Final Enforcement Rule, 71 Fed. Reg. 8,390 (Feb. 16, 2006), amended by HITECH Act Enforcement Interim Final Rule, 74 Fed. Reg. 56,123 (Oct. 30, 2009).

[359] *Id.* at 8425.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act)[360] which was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA)[361] strengthened enforcement mechanisms by providing considerably higher civil penalties,[362] *parens patriae* actions[363] by State attorneys general,[364] and a duty of the Secretary of the HHS to investigate and subsequently impose penalties for violations due to willful neglect.[365]

4.1.2. The Gramm-Leach-Bliley Act Safeguards Rules

§ 501(b) of the Gramm-Leach-Bliley Act (GLBA)[366] requires each federal agency[367] with authority over financial institutions[368] to establish standards "relating to administrative,

[360] Division A, Title XIII and Division B, Title IV of the American Recovery and Reinvestment Act of 2009.

[361] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009)

[362] 42 U.S.C. § 1320d-5(a) as amended by American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009), § 13410(d)(2), implements a differentiated approach regarding minimum penalties, distinguishing whether (A) the person who is in violation "did not know (and by exercising reasonable diligence would not have known)" that such person was in violation (at least $100 for each violation); (B) the violation was "due to reasonable cause and not to willful neglect" (at least $1,000 for each violation); or (C) the violation was due to willful neglect (depending on whether the violation was corrected, at least $10,000 or $50,000 for each violation). The maximum penalty for a single violation is $50,000 and for all violations of an identical provision in a calendar year $1,500,000. *Cf.* HITECH Act Enforcement Interim Final Rule, 74 Fed. Reg. 56,123, 56,127 (Oct. 30, 2009).

[363] The doctrine of *parens patriae* ("parent of his or her country") allows a state to sue on behalf of its citizens when its sovereign or quasi-sovereign interests are implicated and it is not merely litigating the personal claims of its citizens. *See infra* chapter 5.1.7.5 (further discussing the nature of *parens patriae* actions).

[364] The attorney general of a State may bring a civil action to enjoin further violation of the same provision or to obtain damages on behalf of the residents of the State if the interest of one or more of the residents "has been or is threatened or adversely affected." 42 U.S.C. § 1320d-5(d)(1). *Cf. infra* chapter 5.1.1 (discussing liability for HIPAA violations).

[365] *See* 42 U.S.C. § 1320d-5(c).

[366] Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999). For a general introduction see Bernard Shull, *Banking, commerce and competition under the Gramm-Leach-Bliley Act*, 47 ANTITRUST BULL. 25 (2002). For the history of GLBA see Geoffrey M. Connor, *The Financial Services Act of 1999—The Gramm-Leach-Bliley Act*, 71 PA B. ASSN. Q. 29 (2000). *See also* George W. Arnet, III, *The Death of Glass-Steagall and the Birth of the Modern Financial Services Corporation*, 203 N.J. LAW. 42 (2000) (giving information about the background of the Glass-Steagall Act and its development).

technical, and physical safeguards" for the protection of the "security and confidentiality"[369] of their customers' nonpublic personal information.[370]

The purpose of these standards is (1) to insure the security and confidentiality of customer information; (2) to protect against any anticipated threats or hazards to the security or integrity of such information; and (3) to protect against unauthorized access to or use of such information which could result in substantial harm or inconvenience to any customer.[371]

Subsequently, the following agencies have established different security standards: the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), the federal banking agencies (the Office of the Comptroller of the Currency [OCC], the Board of Governors of the Federal Reserve System [Board], the Federal Deposit Insurance Corporation [FDIC], and the Office of Thrift Supervision [OTS]),[372] and the National Credit Union Administration (NCUA).

[367] Pursuant to 15 U.S.C. § 6805(a)(6) (2010), state insurance regulators are also charged with the enforcement of the GLBA's safeguards and privacy provisions insofar as they apply to insurance activities within the state regulators' jurisdiction. Enforcement by state insurance regulators will not be discussed here.

[368] *See* 15 U.S.C. § 6809(3) (generally defining the term "financial institution" as "any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 [12 U.S.C. § 1843(k)]").

[369] Note that 15 U.S.C. § 6801(b) makes no explicit reference to availability of integrity.

[370] Gramm-Leach-Bliley Act § 501(b), 15 U.S.C. § 6801(b). *Cf.* 15 U.S.C. § 6801(a) (stating that it is the policy of the Congress that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to *protect the security and confidentiality of those customers' nonpublic personal information*" (emphasis added)). It is important to note that state laws that provide greater protection than GLBA are not preempted. 15 U.S.C. § 6807(b). *Cf.* Am. Bankers Ass'n v. Lockyer, 541 F.3d 1214 (9th Cir. 2008) (upholding significant portions of the California Financial Information Privacy Act, CAL. FIN. CODE §§ 4050 et seq.), *cert. denied*, 129 S. Ct. 2893 (2009). Note that the California Financial Information Privacy Act does not provide specific obligations with regard to security safeguards. It will therefore not be discussed here.

[371] 15 U.S.C. § 6801(b)(1)-(3).

[372] *Cf.* 12 U.S.C. § 1813(q).

4.1.2.1. The FTC Safeguards Rule

The FTC Safeguards Rule,[373] which became effective in May 2003, applies to all financial institutions over which the FTC has jurisdiction.[374] The material scope of application is limited to "customer information"[375] which is defined as information about consumers[376] who are customers.[377] Pursuant to the FTC Safeguards Rule, financial institutions have to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards."[378] These safeguards have to be "appropriate to [the institution's] size and complexity, the nature and scope of [the institution's] activities, and the sensitivity of any customer information at issue."[379]

[373] FTC Safeguards Rule, 67 Fed. Reg. 36,484 (May 23, 2002) (codified at 16 C.F.R. pt. 314).

[374] 16 C.F.R. § 314.1(b) (2010). Under GLBA, the FTC has jurisdiction over "any other financial institution or other person that is not subject to the jurisdiction of any agency or authority.'' 15 U.S.C. § 6805(a)(7). Therefore, particularly national banks, bank holding companies and savings associations the deposits of which are insured by the FDIC are outside the FTC's jurisdiction. FTC Safeguards Rule, 67 Fed. Reg. 36,484, 36,486 (May 23, 2002). The financial institutions that are within the FTC's jurisdiction include non-depository lenders, consumer reporting agencies, debt collectors, data processors, courier services, retailers that extend credit by issuing credit cards to consumers, personal property or real estate appraisers, check-cashing businesses, and mortgage brokers. *Id.* at 36,485.

[375] *See* 16 C.F.R. § 314.2(b) (defining "customer information" as "any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of [the institution] or [the institution's] affiliates"). 16 C.F.R. § 313.3(n) defines "nonpublic personal information" with reference to "financial information." However, this term is defined very broadly in 16 C.F.R. § 313.3(o)(1), in particular covering any information the institution "obtain[s] about a consumer in connection with providing a financial product or service to [a] consumer."

[376] *See* 15 U.S.C. § 6809(9) (defining "consumer" as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual").

[377] *See* 16 C.F.R. § 313.3(h) (defining "customer" as "a consumer who has a customer relationship with [the financial institution]").

[378] 16 C.F.R. § 314.3(a).

[379] *Id.*

The information security program has to entail (1) the designation of one or more employees to coordinate the program,[380] (2) the implementation of an iterative life cycle approach[381] (similar to the "Plan-Do-Check-Act" [PDCA] process model[382]), and (3) oversight of the institution's service providers[383] by "[t]aking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards" and by "[r]equiring […] service providers by contract to implement and maintain such safeguards."[384]

The iterative life cycle approach to the information security program requires institutions to first perform a risk assessment to identify "reasonably foreseeable" risks to the "security, confidentiality, and integrity"[385] of customer information and to assess the "sufficiency of any safeguards in place to control these risks."[386] Secondly, institutions have to "[d]esign and implement information safeguards to control the risks [they] identify through risk assessment."[387] Thirdly, they have to "regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures."[388] Finally, institutions have to

[380] 16 C.F.R. § 314.4(a).

[381] 16 C.F.R. § 314.4(b), (c), and (e).

[382] For a description of the PDCA-model see ISO & IEC, INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS, ISO/IEC 27001:2005 § 0.2 (2005).

[383] *See* 16 C.F.R. § 314.2(d) (defining "service provider" as "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part").

[384] 16 C.F.R. § 314.4(d).

[385] Note that the Security Rule does not mention "availability." 16 C.F.R. § 314.4(b) only speaks of risks that "could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information." A loss of availability that is not a "destruction" (e.g. a temporary unavailability) is therefore not a risk that has to be considered under the FTC Safeguards Rule.

[386] 16 C.F.R. § 314.4(b). This is equivalent to the "plan"-phase in the PDCA model. *Cf.* ISO & IEC, INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS, ISO/IEC 27001:2005 § 0.2 (2005).

[387] 16 C.F.R. § 314.4(c). This is equivalent to the "do"-phase in the PDCA model.

[388] 16 C.F.R. § 314.4(c). This is equivalent to the "check"-phase in the PDCA model.

"[e]valuate and adjust [their] information security program in light of the results of the testing and monitoring" also taking into account "any material changes to [their] operations or business arrangements" or any other circumstances that may have a material impact on the information security program.

Violations of the FTC Safeguards Rule constitute an unfair and deceptive practice, actionable under § 5(a)(1) of the Federal Trade Commission Act (FTC Act),[389] 15 U.S.C. § 45.[390]

4.1.2.2. The SEC Safeguards Rule

The SEC Safeguards Rule,[391] which became effective in 2000, applies to "[e]very broker, dealer, and investment company, and every investment adviser registered with the [SEC]."[392] The SEC Safeguards Rule only[393] states that these entities have to "adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information" that are "reasonably designed" to achieve the three

[389] Federal Trade Commission Act of 1914, Pub. L. No. 63-203, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. §§ 41-58 (2010)).

[390] *See, e.g.,* In the Matter of James B. Nutter & Co., Decision and Order, FTC Docket No. C-4258 (June 12, 2009), *available at* http://www.ftc.gov/os/caselist/0723108; In the Matter of Premier Capital Lending, Inc., Decision and Order, FTC Docket No. C-4241 (Dec. 10, 2008), *available at* http://www.ftc.gov/os/caselist/0723004; United States v. Am. United Mortgage Co., No. 07C 7064 (N.D. Ill. 2007), *available at* http://www.ftc.gov/os/caselist/0623103; In the Matter of Nations Title Agency, Decision and Order, FTC Docket No. C-4161 (June 19, 2006), *available at* http://www.ftc.gov/os/caselist/0523117/0523117.shtm; In the Matter of Superior Mortgage Corp., Decision and Order, FTC Docket No. C-4153 (Dec. 14, 2005), *available at* http://www.ftc.gov/os/caselist/0523136/0523136.shtm; In the Matter of Nationwide Mortgage Group, Inc., Decision and Order, FTC Docket No. 9319 (Apr. 12, 2005), *available at* http://www.ftc.gov/os/adjpro/d9319; In the Matter of Sunbelt Lending Services, Inc., Decision and Order, FTC Docket No. C-4129 (Jan. 3, 2005), *available at* http://www.ftc.gov/os/caselist/0423153/04231513.shtm. *Cf.* Jane Strachan, *Cybersecurity Obligations*, 20 MAINE B. J. 90, 93 (2005).

[391] Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333 (June 29, 2000) (codified at 17 C.F.R. pt. 248). It should be noted that the SEC issued both, its Privacy Rule and its Safeguards Rule within the same final rule.

[392] 17 C.F.R. § 248.30(a) (2010).

[393] The disposal requirements implemented by the SEC pursuant to FACTA § 216 as part of the SEC Safeguards Rule will be discussed *supra* in the context of FACTA in chapter 4.1.3.2.

general security objectives the Safeguards Rule itself has to fulfill under GLBA.[394] The SEC Safeguards Rule therefore implements a very minimalistic approach.

4.1.2.3. The Interagency Safeguards Guidelines

In furtherance of their obligations under GLBA, the federal banking agencies[395] have jointly issued the "Interagency Safeguards Guidelines."[396] They apply to all banks the respective regulator has jurisdiction over. In substance, the Interagency Safeguards Guidelines are very similar to the FTC Safeguards Rule. Their material scope of application is also limited to "customer information"[397] (i.e. information about consumers who are customers).[398] Pursuant to the Interagency Safeguards Guidelines, banks have to "implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities."[399] The information security program has to be designed to meet the three general

[394] *Id.* As stated above, pursuant to 15 U.S.C. § 6801(b), each federal agency with authority over financial institutions has to establish security standards "(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." *Cf.* Dean William Harvey & Amy White, *Symposium: Exploring Emerging Issues: New Intellectual Property, Information Technology, And Security In Borderless Commerce: The Impact Of Computer Security Regulation On American Companies*, 8 TEX. WESLEYAN L. REV. 505, 522 (2002).

[395] These are the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS). *Cf.* 12 U.S.C. § 1813(q).

[396] Interagency Guidelines Establishing Standards for Safeguarding Customer Information; Final Rule, 66 Fed. Reg. 8,616 (Feb. 1, 2001) (codified at 12 C.F.R. pt. 30, app. B [OCC]; 12 C.F.R. pt. 208, app. D-2, and pt. 225, app. F [Board]; 12 C.F.R. pt. 364, app. B [FDIC]; and 12 C.F.R. pt. 570, app. B [OTS] (2010)).

[397] See Interagency Safeguards Guidelines § I.C.2.e which defines "customer information" identical to the FTC Safeguards Rule. *Cf.* 16 C.F.R. § 314.2(b).

[398] *See* Interagency Security Guidelines § I.C.2.b (using the same definition as 16 C.F.R. § 313.3(h) by referring to 12 C.F.R. §§ 40.3(h) [OCC], 216.3(h) [Board], 332.3(h) [FDIC], and 573.3(h) [OTS]).

[399] Interagency Safeguards Guidelines § II.A.

security objectives laid out in GLBA[400] and the disposal requirement of the Fair and Accurate Credit Transactions Act of 2003.[401] More specifically, for the development and implementation of an information security program, the Interagency Safeguards Guidelines require (1) approval of and oversight over the security program by the board of directors or an appropriate committee of the board,[402] (2) implementation of an iterative life cycle approach,[403] (3) oversight over service providers,[404] and (4) at least annual reporting to the board of directors or an appropriate committee of the board.[405]

Like under the FTC Safeguards Rule, the iterative life cycle approach requires (1) the performance of a risk assessment;[406] (2) the actual implementation of safeguards;[407] (3) regular testing of the information security program;[408] and (4) the evaluation and adjustment of the information security program "in light of any relevant changes in technology, the

[400] Interagency Safeguards Guidelines § II.B.1 to 3 (citing the three objectives provided in 15 U.S.C. § 6801(b)).

[401] The implementation of the disposal requirement of the Fair and Accurate Credit Transactions Act of 2003 will be discussed in chapter 4.1.3.2.

[402] Interagency Safeguards Guidelines § III.A. *Cf. also id.* § I.C.a (defining "board of directors," in the case of a branch or agency of a foreign bank, as "the managing official in charge of the branch or agency").

[403] *Cf.* Interagency Safeguards Guidelines § III.B, C, and E. FTC: 16 C.F.R. § 314.4(b), (c), and (e).

[404] Interagency Safeguards Guidelines § III.D (stating that "[e]ach bank shall: 1. Exercise appropriate due diligence in selecting its service providers; 2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and 3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations […]"). The last requirement goes beyond what is mandated by the FTC Safeguards Rule. *Cf.* 16 C.F.R. § 314.4(d).

[405] Interagency Safeguards Guidelines § III.F (stating that the report should "describe the overall status of the information security program and the bank's compliance with these Guidelines" and "discuss […] security breaches or violations and management's responses").

[406] Interagency Safeguards Guidelines § III.F.

[407] Interagency Safeguards Guidelines § III.C.1, 2, 4.

[408] Interagency Safeguards Guidelines § III.C.3, E..

sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements."[409]

In contrast to the FTC Safeguards Rule, the Interagency Safeguards Guidelines provides a list of security measures that have to be considered and subsequently implemented if the bank concludes that they are "appropriate." These are (a) logical access controls, (b) physical access controls, (c) encryption, (d) change control procedures for information systems, (e) dual control procedures, segregation of duties, and employee background checks, (f) intrusion detection systems and procedures, (f) incident response programs, and (f) measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards or technological failures.[410] Lastly, the Interagency Safeguards Guidelines provide two mandatory safeguards: staff training to implement the information security program[411] and measures for the disposal of customer information as well as information derived from consumer credit reports.[412]

In a reaction to the mounting threat of "identity theft,"[413] the federal banking agencies have issued the "Interagency Incident Response Guidance"[414] to further specify the requirements

[409] Interagency Safeguards Guidelines § III.E.

[410] *See* Interagency Safeguards Guidelines § III.C.1.a-h.

[411] Interagency Safeguards Guidelines § III.C.2.

[412] This requirement will be discussed in the context of the Fair and Accurate Credit Transactions Act of 2003. *See supra* chapter 4.1.3.2.

[413] *See supra* chapter 4.1.10.1 (extensively discussing the misconception of "identity theft").

[414] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005) (codified at 12 C.F.R. pt. 30, app. B, supp. A [OCC], 12 C.F.R. pt. 208, app. D-2, supp. A and pt. 225, app. F, supp A [Board]; 12 C.F.R. pt. 364, app. B, supp. A [FDIC]; and 12 C.F.R. pt. 570, app. B, supp. A [OTS]). *See id.* at 15,751 (stating that "[t]his Guidance interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and the Interagency Guidelines Establishing Information Security Standards").

for incident response programs. “At a minimum,” an incident response program should contain procedures for (1) assessing the nature and scope of an incident; (2) notifying the bank’s primary Federal regulator if the incident involved unauthorized access to or use of sensitive customer information;[415] (3) notifying appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate attention; (4) taking appropriate steps to contain and control the incident to prevent further damages; and (5) notifying customers when warranted.[416] In light of this interpretive guidance by the federal banking agencies, incident response programs should also be considered a mandatory safeguard.

4.1.2.4. The NCUA Safeguards Guidelines

The National Credit Union Administration (NCUA) adopted its own Safeguards Guidelines[417] and Incident Response Guidance,[418] covering federally-insured credit unions.[419] The NCUA Safeguards Guidelines and the NCUA Incident Response Guidance are, however, for all practical purposes identical to the Interagency Safeguards Guidelines and the Interagency Incident Response Guidance.[420]

[415] *See* Interagency Incident Response Guidance § III.A.1 (defining “sensitive customer information” as “a customer’s name, address, or telephone number, in conjunction with the customer’s social security number, driver’s license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer’s account”).

[416] Interagency Incident Response Guidance § II.A.1.a-d. For a discussion of data security breach notification requirements under GLBA see *supra* chapter 6.2.5.

[417] Guidelines for Safeguarding Member Information; Final Rule, 66 Fed. Reg. 8,152 (Jan. 30, 2001) (codified at 12 C.F.R. pt. 748, app. A (2010)).

[418] Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice; Final Rule, 70 Fed. Reg. 22,764 (May 2, 2005) (codified at 12 C.F.R. § 748.0 and pt. 748, app. B).

[419] *See* NCUA Safeguards Guidelines § I.A (stating that “[t]he Guidelines apply to member information maintained by or on behalf of federally-insured credit unions”).

[420] The only differences are of a linguistic nature.

4.1.2.5. Enforcement

The FTC Safeguards Rule, the SEC Safeguards Rule, the Interagency Safeguards Guidelines, and the NCUA Safeguards Guidelines are all to be enforced by the respective regulatory agency by bringing an action against the entity in question.[421] Courts have consistently held that GLBA does not provide a private right of action.[422]

4.1.3. Safeguard Requirements under the Fair Credit Reporting Act

In the United States, consumer reporting agencies assemble and evaluate data that relates to a consumer's creditworthiness, credit standing, credit capacity, character, and general reputation. This information is being sold to third parties in particular in order to allow them to better assess a consumer's creditworthiness.[423]

The integrity of that data is therefore of great importance to the individuals concerned as inaccurate data can result in less favorable credit terms or might even make it impossible to obtain a loan.[424]

[421] *See* 15 U.S.C. § 6805(a) (2010).

[422] For a recent decision see *In re* Lentz, 405 B.R. 893, 899 (Bankr. N.D. Ohio 2009) (citing Dunmire v. Morgan Stanley DW Inc., 475 F.3d 956 (8th Cir. 2007); *In re* Southhall, No. 07-00115, 2008 WL 5330001, at *4 (Bankr. N.D. Ala. Dec. 18, 2008); and *In re* French, 401 B.R. 295, 309 (Benkr. E.D. Tenn. 2009)).

[423] In the United States, the "Big Three" nationwide credit reporting agencies, Equifax, TransUnion, and Experian (formerly TRW), as of 2004, keep information on about 200 million consumers and issue more than 1.5 billion consumer reports a year. The data in these files is provided on a voluntary basis by about 30,000 data furnishers. FEDERAL TRADE COMM'N [FTC], FTC REPORT TO CONGRESS UNDER SECTIONS 318 AND 319 OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003, at 8 (2004), *available at* http://www.ftc.gov/reports/facta/041209factarpt.pdf.

[424] *Cf.* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 25 et seq. (2000).

Furthermore, consumers also have an interest in the confidentiality of this data that potentially reveals information traditionally considered private to the individual concerned and/or would allow criminals to conduct impersonation fraud.[425]

In the United States, these issues are primarily addressed by the Fair Credit Reporting Act (FCRA)[426] as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA).[427]

The FCRA protects the confidentiality of consumer[428] credit information by (1) mandating identification and authentication procedures for the provision of information to third parties (see chapter 4.1.3.1); and (2) by requiring the FTC, the SEC, the federal banking agencies,[429] and the National Credit Union Administration (NCUA) to implement specific rules for the disposal of consumer credit information (see chapter 4.1.3.2).

The FCRA also mandates specific security controls to protect the integrity (and accuracy) of consumer credit information by (1) requiring reasonable procedures to assure accuracy of the information reported by consumer reporting agencies (chapter 4.1.3.3); (2) requiring

[425] Besides 15 U.S.C. § 1681c, there are few limits on the information that might be kept in a consumer report, as long as it is complete, accurate, and not obsolete. *Cf.* FTC Official Staff Commentary § 607 item 6, 16 C.F.R. pt. 600, app. The "Big Three" nationwide credit reporting agencies keep the following information: personal identifiers (in particular name, address, and Social Security number), credit account information (detailed information on each "trade line" or credit account in a consumer's credit files), public record information, credit scores, inquiries made about a consumer's credit history, and any consumer statements. Robert B. Avery et al., *An Overview of Consumer Data and Credit Reporting*, FED. RES. BULL. (Board of Governors of the Federal Reserve System, Washington, D.C.), Feb. 2003, at 47, *available at* http://www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf.

[426] Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114 (1970) (codified as amended at 15 U.S.C. § 1681).

[427] Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 117 Stat. 1952 (2003) (amending 15 U.S.C. §§ 1681-1681x, 20 U.S.C. §§ 9701-08, and 31 U.S.C. § 5318).

[428] *See* 15 U.S.C. § 1681a(c) (2010) (stating that the term "consumer" means an individual).

[429] The Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS). *Cf.* 12 U.S.C. § 1813(q).

reasonable policies and procedures to assure the integrity and accuracy of information furnished to consumer reporting agencies (chapter 4.1.3.4); and (3) attempting to prevent impersonation fraud (chapters 4.1.3.5 and 4.1.3.6). This is significant because a criminal who succeeds in defrauding a creditor by impersonating a consumer pollutes the consumer's credit information with information pertaining to the fraud-related transaction—that is if the impersonation fraud is not detected.

4.1.3.1. Identification and Authentication Procedures

Under FCRA § 604,[430] a consumer reporting agency[431] may only furnish a consumer report[432] under specific circumstances, which include having reason to believe that the person requesting the report has legitimate business interests in connection with a business transaction that is initiated by the consumer.[433] To limit the furnishing of consumer reports to these circumstances, a consumer reporting agency is obligated under FCRA § 607[434] to "maintain reasonable procedures" that "require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that

[430] 15 U.S.C. § 1681b(a).

[431] *See* 15 U.S.C. § 1681a(f) (defining "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties […]"). This also includes "resellers." *See* 15 U.S.C. § 1681a(u).

[432] *See* 15 U.S.C. § 1681a(d)(1) (defining "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under [15 U.S.C. § 1681b]").

[433] *See* 15 U.S.C. § 1681b(a)(3)(F)(i).

[434] 15 U.S.C. § 1681e.

the information will be used for no other purpose."[435] These procedures can be described as identification procedures.[436] A consumer reporting agency must also have a system to *verify* that it is dealing with a legitimate business having a "permissible purpose" for the information.[437] This can be described as a weak[438] authentication system.[439] Subsequently, it may only furnish the report if it does not have "reasonable grounds for believing" that the consumer report will be used for impermissible purposes.[440]

4.1.3.2. FACTA Disposal Rules

To protect the confidentiality of consumer credit information, FACTA § 216 added § 628 to the FCRA, mandating that the FTC, the SEC, the federal banking agencies, and the NCUA issue consistent and comparable[441] rules for the disposal of consumer credit information.[442] Subsequently, the FTC, the SEC, and the NCUA promulgated separate and the federal banking agencies a joint rule.[443]

[435] 15 U.S.C. § 1681e(a).

[436] *See* NIST, AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK, SPECIAL PUBLICATION 800-12, at 181 (1995), *available at* http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (defining "identification" as "the means by which a user *provides* a claimed identity to the system").

[437] *See* 15 U.S.C. § 1681e(a); FTC Official Staff Commentary § 607 item 2A, 16 C.F.R. pt. 600, app.

[438] *Cf. id.* (stating that "adequate verification will vary with the circumstances").

[439] *See* NIST, AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK, SPECIAL PUBLICATION 800-12, at 181 (1995), *available at* http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (defining "authentication" as "the means of establishing the *validity* of this claim [of identity]").

[440] 15 U.S.C. § 1681e(a).

[441] *See* 15 U.S.C. § 1681w(a)(2)(A) (mandating cooperation between the agencies). The agencies were also obligated to ensure that their regulations are consistent with the requirements and regulations issued pursuant GLBA. 15 U.S.C. § 1681w(a)(2)(B).

[442] FCRA § 628, 15 U.S.C. § 1681w(a)(1).

[443] The SEC, the federal banking agencies, and the NCUA have implemented FACTA § 216 by respectively amending the SEC Safeguards Rule, the Interagency Safeguards Guidelines, and the NCUA Safeguards Rule which were issued to implement GLBA § 501(b). *See supra.* However, because the FTC's jurisdiction under FACTA is broader than under the GLBA, the FTC has chosen to adopt a separate rule to implement FACTA

The FTC Disposal Rule[444] has a very broad scope as it applies to any person over whom the FTC has jurisdiction that, for a business purpose, maintains or otherwise possesses consumer information.[445] The Rule requires covered entities to properly dispose[446] of consumer information by "taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[447] The FTC Disposal Rule further provides examples of "reasonable measures": (1) implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers,[448] or that require the destruction or erasure of electronic media;[449] (2) when outsourcing the disposal, taking appropriate measures to determine the competency and integrity of the potential disposal company (e.g. reviewing an independent audit, requiring certification by a recognized third party);[450] or (3) implementing and monitoring compliance with policies and

§ 216. *See* Disposal of Consumer Report Information and Records; Final Rule, 69 Fed. Reg. 68,690, 68,690 (Nov. 24, 2004).

[444] Disposal of Consumer Report Information and Records; Final Rule, 68 Fed. Reg. 68,690 (Nov. 24, 2004) (codified at 16 C.F.R. pt. 682).

[445] 16 C.F.R. § 682.2(b). *See* 16 C.F.R. 682.1(b) (defining "consumer information" as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.").

[446] *See* 16 C.F.R. 682.1(c) (defining "dispose" as "(1) The discarding or abandonment of consumer information, or (2) The sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.").

[447] 16 C.F.R. § 682.3(a)

[448] 16 C.F.R. § 682.3(b)(1).

[449] 16 C.F.R. § 682.3(b)(2). Files that have been "erased" using regular delete functionality can be easily restored. Electronic media should therefore be destroyed, degaussed, or at least overwritten multiple times. *Cf.* DAN FARMER & WIETSE VENEMA, FORENSIC DISCOVERY 145 et seq. (2004).

[450] 16 C.F.R. § 682.3(b)(3).

procedures that protect against unauthorized or unintentional disposal of consumer information.[451]

The SEC Disposal Rule[452] implements FACTA's disposal requirements by amending the SEC Safeguards Rule.[453] It requires covered entities[454] that maintain or otherwise possess "consumer report information"[455] for a business purpose to "properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[456] In contrast to the FTC Disposal Rule, the SEC Disposal Rule does not provide any further guidance for what constitutes a "reasonable measure."

The Interagency Disposal Rule[457] promulgated by the federal banking agencies implements FACTA's disposal requirements by amending the Interagency Safeguards Guidelines.[458] The amended Guidelines require a covered entity, irrespective of the outcome of the risk

[451] 16 C.F.R. § 682.3(b)(4).

[452] Disposal of Consumer Report Information; Final Rule, 69 Fed. Reg. 71,322 (Dec. 8, 2004) (codified at 17 C.F.R. pt. 248).

[453] Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333 (June 29, 2000) (codified at 17 C.F.R. pt. 248). *Cf. supra* chapter 4.1.2.2 (describing the SEC Safeguards Rule in detail).

[454] Note that the personal scope of application of the SEC Disposal Rule is narrower than the SEC Safeguards Rule in the sense that it exempts "notice-registered broker-dealers" and broader in the sense that it also covers "transfer agents." *See* 17 C.F.R. § 248.30(b)(2), (b)(1)(iv), and (b)(1)(v).

[455] *See* 17 C.F.R. § 248.30(b)(1)(ii) (defining "consumer report information" identical to the term "consumer information" as defined in the FTC Disposal Rule, 16 C.F.R. § 682.1(b)).

[456] 17 C.F.R. § 248.30(b)(2)(i).

[457] Interagency Disposal Rule, 69 Fed. Reg. 77610 (Dec. 28, 2004) (codified at 12 C.F.R. pts. 30 and 40 [OCC], 12 C.F.R. pts. 208, 211, 222, and 225 [Board], 12 C.F.R. pts. 334 and 364 [FDIC], 12 C.F.R. pts. 568, 570, and 571 [OTS]).

[458] Interagency Guidelines Establishing Standards for Safeguarding Customer Information; Final Rule, 66 Fed. Reg. 8,616 (Feb. 1, 2001). *Cf. supra* chapter 4.1.2.3 (describing the Interagency Safeguards Guidelines in detail).

assessment performed in accordance with the Guidelines,[459] to "[d]evelop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of customer information and consumer information."[460]

The NCUA Disposal Rule[461] mirrors the Interagency Disposal Rule and implemented FACTA's disposal requirements by amending the NCUA Safeguards Guidelines.[462]

The FTC Disposal Rule, the SEC Disposal Rule, the Interagency Disposal Rule, and the NCUA Disposal Rule are all subject to the enforcement by the respective regulatory agency which may bring an action against the entity in question.[463]

4.1.3.3. Consumer Reporting Agency Procedures to Assure Accuracy

Under FCRA § 697(b),[464] consumer reporting agencies must follow "reasonable procedures to assure maximum possible accuracy of the information" when preparing a consumer report. "Reasonable procedures" are those that a reasonably prudent person would undertake under

[459] *See* Interagency Safeguards Guidelines III.B.

[460] Interagency Safeguards Guidelines III.C.4. Note that the term "consumer information" as defined in Interagency Safeguards Guidelines I.C.2.b. is identical to the definition of the term "consumer information" in the FTC Disposal Rule, 16 C.F.R. § 682.1(b) and the term "consumer report information" in the SEC Disposal Rule, 17 C.F.R. § 248.30(b)(ii). The term "customer information," on the other hand, only covers information about customers but is broader in the sense that it does not only cover personal information derived from a credit report but all "any record containing nonpublic personal information […] about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the bank." Interagency Safeguards Guidelines III.C.2.e.

[461] NCUA Disposal Rule, 69 Fed. Reg. 69269 (Nov. 29, 2004) (codified at 12 C.F.R. pts. 717 and 748).

[462] Guidelines for Safeguarding Member Information; Final Rule, 66 Fed. Reg. 8,152 (Jan. 30, 2001). *Cf. supra* chapter 4.1.2.4 (describing the NCUA Safeguards Guidelines in detail).

[463] For a recent FTC enforcement action under Federal Trade Commission Act § 5(a)(1), 15 U.S.C. § 45, see United States v. Am. United Mortgage Co., No. 07C 7064 (N.D. Ill. 2007) (stipulated judgment and final order requiring defendant to pay $50,000 for having left consumer information in and around an unsecured dumpster). *See also* In the Matter of Nations Title Agency, Decision and Order, FTC Docket No. C-4161 (June 19, 2006), *available at* http://www.ftc.gov/os/caselist/0523117/0523117.shtm;

[464] 15 U.S.C. § 1681e(b).

the circumstances.[465] With regard to "automatic data processing equipment," the FTC Official Staff Commentary states that this requires the adoption of "[r]easonable security procedures […] to minimize the possibility that computerized consumer information will be stolen or altered by either authorized or unauthorized users of the information system."[466]

4.1.3.4. Furnisher Procedures to Assure Accuracy

FCRA § 623(e), as amended by FACTA § 312, mandates that the federal banking agencies (OCC, Board of Governors of the Federal Reserve System, FDIC, and OTS), the NCUA, and the FTC (1) "establish and maintain guidelines" for use by each person that furnishes information to consumer reporting agencies (furnisher) "regarding the accuracy and integrity of the information relating to consumers";[467] and (2) prescribe regulations requiring each furnisher "to establish reasonable policies and procedures for implementing the guidelines."[468]

The Furnishers Rule[469] subsequently promulgated by the agencies became effective on July 1, 2010[470] and requires furnishers to "establish and implement reasonable written policies and

[465] *See, e.g.,* Spence v. TRW, Inc., 92 F.3d 380, 383 (6th Cir. 1996) (citing Bryant v. TRW, Inc., 689 F.2d 72, 78 (6th Cir. 1982)). *Cf. also* CHI CHI WU & ELISABETH DE ARMOND, FAIR CREDIT REPORTING 107 et seq. (6th ed. 2006).

[466] FTC Official Staff Commentary § 607 item 3C, 16 C.F.R. pt. 600, app.

[467] 15 U.S.C. § 1681s-2(e)(1)(A).

[468] 15 U.S.C. § 1681s-2(e)(1)(B).

[469] Procedures To Enhance the Accuracy and Integrity of Information Furnished to Consumer Reporting Agencies Under Section 312 of the Fair and Accurate Credit Transactions Act; Final Rule, 74 Fed. Reg. 31,484 (July 1 2009) (codified at 12 C.F.R. pt. 41 [OCC], 12 C.F.R. pt. 222 [Board], 12 CFR pt. 334 [FDIC], 12 C.F.R. pt. 571 [OTS], 12 C.F.R. pt. 717 [NCUA], 16 C.F.R. pt. 660 [FTC]). *See generally* CHI CHI WU, FAIR CREDIT REPORTING 107 et seq. (Supp. 2009).

[470] *Id.* at 31,484.

procedures" regarding the "accuracy"[471] and "integrity"[472] of the information relating to consumers that they furnish to a consumer reporting agency.[473] In developing the policies and procedures, furnishers have to consider the guidelines and incorporate those that are "appropriate."[474] The Rule further provides that the policies and procedures "must be appropriate to the nature, size, complexity, and scope of each furnisher's activities"[475] and must be reviewed and updated "as necessary to ensure their continued effectiveness."[476]

The guidelines are structured in three parts: (1) nature, scope, and objectives;[477] (2) establishing and implementing policies and procedures;[478] and, most significantly, (3) specific

[471] *See* 12. C.F.R. § 41.41(a) (OCC), 12 C.F.R. § 222.41(a) (Board), 12 CFR § 334.41(a) (FDIC), 12 C.F.R. § 571.41(a) (OTS), 12 C.F.R. § 717.41(a) (NCUA), 16 C.F.R. § 660.2(a) (FTC) (stating that "[a]ccuracy means that information that a furnisher provides to a consumer reporting agency about an account or other relationship with the consumer correctly: (1) Reflects the terms of and liability for the account or other relationship; (2) Reflects the consumer's performance and other conduct with respect to the account or other relationship; and (3) Identifies the appropriate consumer.").

[472] *See* 12. C.F.R. § 41.41(e) (OCC), 12 C.F.R. § 222.41(e) (Board), 12 CFR § 334.41(e) (FDIC), 12 C.F.R. § 571.41(e) (OTS), 12 C.F.R. § 717.41(e) (NCUA), 16 C.F.R. § 660.2(e) (FTC) (stating that "[i]ntegrity means that information that a furnisher provides to a consumer reporting agency about an account or other relationship with the consumer: (1) Is substantiated by the furnisher's records at the time it is furnished; (2) Is furnished in a form and manner that is designed to minimize the likelihood that the information may be incorrectly reflected in a consumer report; and (3) Includes the information in the furnisher's possession about the account or other relationship that [the respective agency] has: (i) Determined that the absence of which would likely be materially misleading in evaluating a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living; and (ii) Listed in section I.(b)(2)(iii) of [the guidelines].").

[473] 12. C.F.R. § 41.42(a) (OCC), 12 C.F.R. § 222.42(a) (Board), 12 CFR § 334.42(a) (FDIC), 12 C.F.R. § 571.42(a) (OTS), 12 C.F.R. § 717.42(a) (NCUA), 16 C.F.R. § 660.3(a) (FTC).

[474] *See* 12. C.F.R. § 41.42(c) (OCC), 12 C.F.R. § 222.42(c) (Board), 12 CFR § 334.42(c) (FDIC), 12 C.F.R. § 571.42(c) (OTS), 12 C.F.R. § 717.42(c) (NCUA), 16 C.F.R. § 660.3(c) (FTC).

[475] *See* 12. C.F.R. § 41.42(a) (OCC), 12 C.F.R. § 222.42(a) (Board), 12 CFR § 334.42(a) (FDIC), 12 C.F.R. § 571.42(a) (OTS), 12 C.F.R. § 717.42(a) (NCUA), 16 C.F.R. § 660.3(a) (FTC).

[476] *See* 12. C.F.R. § 41.42(c) (OCC), 12 C.F.R. § 222.42(c) (Board), 12 CFR § 334.42(c) (FDIC), 12 C.F.R. § 571.42(c) (OTS), 12 C.F.R. § 717.42(c) (NCUA), 16 C.F.R. § 660.3(c) (FTC).

[477] To determine the nature and scope of the required policies and procedures, a furnisher should consider "[t]he types of business activities in which the furnisher engages; (2) The nature and frequency of the information the furnisher provides to consumer reporting agencies; and (3) The technology used by the furnisher to furnish information to consumer reporting agencies." The identified objectives are "[t]o furnish information […] that is accurate [and] has integrity," to "conduct reasonable investigations of consumer disputes," and to "update the information it furnishes as necessary." *See* Furnishers Guidelines I.a.

components of policies and procedures. The latter part lists a number of components that are to be addressed "as appropriate." The components are either focused on preventing processing or transmission errors,[479] designed to detect or correct inaccuracies resulting from errors or impersonation fraud[480] or are of a very general nature.[481] However, none of the components specifically requires a furnisher to verify the identities of the consumers to which the information supposedly relates to.

The Furnishers Rule is subject to the enforcement by the FTC, the federal banking agencies, and the NCUA.[482] Private enforcement is not available.[483]

4.1.3.5. Identity Theft Red Flag Requirements

The Identity Theft Red Flags and Address Discrepancies Rule[484] (hereinafter *Red Flags Rule*) jointly issued pursuant to FACTA §§ 114 and 315[485] by the federal banking agencies, the

[478] In establishing and implementing its policies and procedures, a furnisher should: (a) "[i]dentify practices or activities of the furnisher that can compromise the accuracy or integrity of information furnished to consumer reporting agencies […]"; (b) "[e]valuate the effectiveness of existing policies and procedures […]"; and (c) "[e]valuate the effectiveness of specific methods (including technological means) [used to furnish information]." *See* Furnishers Guidelines I.b.

[479] *See* Furnishers Guidelines III.b (using standard data reporting formats); *id.* III.g (furnishing information following acquisitions or transfers of accounts in a manner that prevents errors); *id.* III.j (designing means of communication with consumer reporting agencies to prevent errors); *id.* III.k (providing sufficient identifying information to enable the consumer reporting agency properly to identify the consumer).

[480] *See* Furnishers Guidelines III.c (maintaining records for a reasonable period of time); *id.* III.d (implementing appropriate internal accuracy and integrity controls such as verifying random samples); *id.* III.h (updating information in the furnisher's records to avoid furnishing inaccurate information); *id.* III.i (conducting reasonable investigations of disputes).

[481] *See* Furnishers Guidelines III.a (establishing and implementing an appropriate system for furnishing information); *id.* III.e (staff training); *id.* III.f (oversight of relevant service providers); *id.* III.l (conducting a periodic evaluation of its own practices); *id.* III.m (complying with other requirements under the FCRA).

[482] *See* 15 U.S.C. § 1681s(a) and (b). *Cf.* CHI CHI WU & ELISABETH DE ARMOND, FAIR CREDIT REPORTING 379 et seq. (6th ed. 2006) (providing an extensive discussion of the enforcement powers of the respective agencies).

[483] *See* 15 U.S.C. § 1681s-2(c)(2) and (d). *Cf.* CHI CHI WU & ELISABETH DE ARMOND, FAIR CREDIT REPORTING 184 (6th ed. 2006) (noting that the apparent import of the standards of accuracy for furnishers can be misleading since they cannot be enforced by consumers). *Cf.* chapter 5.1.3 (discussing the immunity from tort liability under 15 U.S.C. § 1681h(e)).

NCUA, and the FTC prescribes (1) duties for financial institutions and creditors regarding the detection, prevention, and mitigation of impersonation fraud (described below); and (2) duties for card issuers regarding changes of address (described in chapter 4.1.3.6).[486]

The Red Flags Rule requires financial institutions and creditors that offer or maintain "covered accounts"[487] to develop and implement a written "Identity Theft Prevention Program" that has to be designed to "detect, prevent, and mitigate" impersonation fraud in connection with "the opening of a covered account or any existing covered account."[488] The Rule provides some flexibility by stating that the program must be appropriate to "the size

[484] Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule, 72 Fed. Reg. 63,718 (Nov. 9, 2007) (codified at 12 C.F.R. pt. 41 [OCC], 12 C.F.R. pt. 222 [Board], 12 C.F.R. pts. 334 and 364 [FDIC], 12 C.F.R. pt. 571 [OTS], 12 C.F.R. pt. 717 [NCUA], 16 C.F.R. pt. 681 [FTC]).

[485] 15 U.S.C. §§ 1681c(h), 1681m(e). 15 U.S.C. §§ 1681c(h) states that a consumer reporting agency has to notify discrepancies between the address stored in the consumer's file and an address contained in a consumer report request to the requestor (user). The Rule mandates that users develop and implement reasonable policies and procedures designed to enable them to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when he receives a notice of address discrepancy from the consumer reporting agency. *See* 12 C.F.R. §§ 41.82(c) [OCC], 222.82(c) [Board], 334.82(c) [FDIC], 571.82(c) [OTS], 717.82(c) [NCUA], and 16 C.F.R. § 681.1(c) [FTC]. As this requirement is intended to prevent accidental incorrect use of a consumer report and does not directly relate to information security, it will not be discussed here. The Rule also requires users to furnish an address they have reasonably confirmed as accurate to the consumer reporting agency. This certainly enhances the accuracy of consumer information but can nonetheless not be considered a security measure and will therefore not be discussed here either. *See* 12 C.F.R. §§ 41.82(d) [OCC], 222.82(d) [Board], 334.82(d) [FDIC], 571.82(d) [OTS], 717.82(d) [NCUA], and 16 C.F.R. § 681.1(d) [FTC].

[486] The Red Flags Rule also requires users of consumer reports to "develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy [from the consumer reporting agency]." 12 C.F.R. §§ 41.82(c) [OCC], 222.82(c) [Board], 334.82(c) [FDIC], 571.82(c) [OTS], 717.82(c) [NCUA], and 16 C.F.R. § 681.1(c) [FTC].

[487] *See* 12 C.F.R. §§ 41.90(b)(3) [OCC], 222.90(b)(3) [Board], 334.90(b)(3) [FDIC], 571.90(b)(3) [OTS], 717.90(b)(3) [NCUA], and 16 C.F.R. § 681.2(b)(3) [FTC] (defining "covered account" as "(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.").

[488] 12 C.F.R. §§ 41.90(d) [OCC], 222.90(d) [Board], 334.90(d) [FDIC], 571.90(d) [OTS], 717.90(d) [NCUA], and 16 C.F.R. § 681.2(d) [FTC].

and complexity" of the covered entity and "the nature and scope of its activities."[489] More specifically, the Rule mandates that the program includes "reasonable policies and procedures" to (i) define relevant "Red Flags"[490] for the covered accounts and incorporate those into its program; (ii) detect Red Flags that have been incorporated into the program; (iii) respond appropriately to any Red Flags that are detected to prevent and mitigate impersonation fraud; (iv) ensure the program (including the defined Red Flags) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the covered entity from impersonation fraud.[491] Furthermore, the Rule mandates continued administration of the program which requires (1) to obtain approval of the initial written program from the board of directors[492] or an appropriate committee thereof; (2) to involve the board of directors, an appropriate committee thereof, or a designated senior manager in the oversight, development, implementation, and administration of the program; (3) to train staff, as necessary, to effectively implement the program; and (4) to exercise appropriate and effective oversight of service provider arrangements.[493] The Rule also provides detailed

[489] *Id.*

[490] *See* 12 C.F.R. §§ 41.90(b)(9) [OCC], 222.90(b)(9) [Board], 334.90(b)(9) [FDIC], 571.90(b)(9) [OTS], 717.90(b)(9) [NCUA], and 16 C.F.R. § 681.2(b)(9) [FTC] (defining "Red Flag" as "a pattern, practice, or specific activity that indicates the possible existence of identity theft").

[491] 12 C.F.R. §§ 41.90(d)(2) [OCC], 222.90(d)(2) [Board], 334.90(d)(2) [FDIC], 571.90(d)(2) [OTS], 717.90(d)(2) [NCUA], and 16 C.F.R. § 681.2(d)(2) [FTC]. This is very similar to a common incident response methodology that consists of the steps prepare, detect, contain, eradicate, recover, and follow-up (containment, eradication, and recovery being combined in (iii)). *Cf.* E. EUGENE SCHULTZ & RUSSELL SHUMWAY, INCIDENT RESPONSE: A STRATEGIC GUIDE TO HANDLING SYSTEM AND NETWORK SECURITY BREACHES 45 (2001). *See also* Michael Vangelos, *Managing the Response to a Computer Security Incident, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 2989, 2992 et seq. (Harold F. Tipton & Micki Krause eds., 6th ed. 2007).

[492] *See* 12 C.F.R. §§ 41.90(b)(2) [OCC], 222.90(b)(2) [Board], 334.90(b)(2) [FDIC], 571.90(b)(2) [OTS], and 16 C.F.R. § 681.2(b)(2) (stating that "board of directors includes: (i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and (ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management"); 12 C.F.R. § 717.90(b)(2) [NCUA] (defining "board of directors" as "a federal credit union's board of directors").

[493] 12 C.F.R. §§ 41.90(e) [OCC], 222.90(e) [Board], 334.90(e) [FDIC], 571.90(e) [OTS], 717.90(e) [NCUA], and 16 C.F.R. § 681.2(e) [FTC].

Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation[494] which a covered entity must consider and integrate into its program to the extent "appropriate."[495]

4.1.3.6. Change of Address Procedures for Card Issuers

The second security control mandated by Identity Theft Red Flags and Address Discrepancies Rule concerns duties for card issuers in the case of a change of address. A specific type of impersonation fraud related to credit and debit cards is perpetrated by falsifying a change of address notification and then requesting that an additional or replacement card be sent to the new address that has been provided by the perpetrator. To mitigate this risk, the Rule requires a "card issuer"[496] to establish and implement "reasonable policies and procedures to assess the validity of a change of address" if it receives notification of a change of address for a consumer's debit or credit card account and, within 30 days, receives a request for an additional or replacement card for the same account.[497] Under these circumstances, a card issuer may only issue the new card if (1) he notifies the cardholder of the request and provides him with a reasonable means of promptly reporting incorrect address changes, or (2) otherwise assesses the validity of the change of address.[498]

[494] 12 C.F.R. pt. 41, app. J [OCC], pt. 222, app. J [Board], pt. 334, app. J [FDIC], pt. 571, app. J [OTS], pt. 717, app. J [NCUA], and 16 C.F.R. pt. 681, app. A [FTC]. A detailed discussion of the Guidelines is omitted here as they relate to fraud and only indirectly to information security.

[495] 12 C.F.R. §§ 41.90(f) [OCC], 222.90(f) [Board], 334.90(f) [FDIC], 571.90(f) [OTS], 717.90(f) [NCUA], and 16 C.F.R. § 681.2(f) [FTC].

[496] *See* 12 C.F.R. §§ 41.91(a) [OCC], 222.91(a) [Board], 334.91(a) [FDIC], 571.91(a) [OTS], 717.91(a) [NCUA], and 16 C.F.R. § 681.3(a) [FTC] (defining "card issuer" as a financial institution or creditor that issues a debit or credit card).

[497] 12 C.F.R. §§ 41.91(c) [OCC], 222.91(c) [Board], 334.91(c) [FDIC], 571.91(c) [OTS], 717.91(c) [NCUA], and 16 C.F.R. § 681.3(c) [FTC].

[498] *Id.*

4.1.3.7. Enforcement

All of the regulatory obligations under FCRA discussed above are subject to public enforcement by the FTC,[499] the SEC, the federal banking agencies (OCC, Board of Governors of the Federal Reserve System, FDIC, and OTS), and the NCUA.[500] Furthermore, if the chief law enforcement officer of a state, or an official or agency designated by a state, has reason to believe that a person has violated or is violating the FCRA, specifically the regulatory obligations discussed above, the official may bring (1) an action to enjoin the violation;[501] and (2) a *parens patriae* action to recover statutory damages of not more than $1,000 for each willful or negligent violation.[502]

4.1.4. The Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act of 1998 (COPPA)[503] requires that the FTC promulgates regulations that mandate the establishment and maintenance of "reasonable procedures" to protect the "confidentiality, security, and integrity"[504] of "personal

[499] *See, e.g.,* Stipulated Final Judgment and Order of Civil Penalties, Permanent Injunction, and Other Equitable Relief, U.S. v. Choicepoint, Inc. (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf (defendant agreed to pay $10 million in civil penalties and $5 million in consumer redress after financial records of more than 163,000 consumers have been compromised, *inter alia*, in violation of 15 U.S.C. § 1681e(a) [see chapter 4.1.3.1]). *Cf.* Joel B. Hanson, *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints against Businesses Victimized by Consumer Information Security Breaches*, 4 SHIDLER J. L. COM. & TECH. 11 (2008).

[500] *See* 15 U.S.C. § 1681s(a) and (b). *Cf.* CHI CHI WU & ELISABETH DE ARMOND, FAIR CREDIT REPORTING 379 et seq. (6th ed. 2006) (providing an extensive discussion of the enforcement powers of the respective agencies).

[501] 15 U.S.C. § 1681s(c)(1)(A).

[502] 15 U.S.C. § 1681s(c)(1)(B)(iii). Note that the possibility to recover actual damages (suffered in the event of a security breach) by means of a private action under 15 U.S.C. §§ 1681n, 1681o or a *parens patriae* action under 15 U.S.C. § 1681s(c)(1)(B)(i) is discussed *infra* in the appropriate context under chapter 5.1.3.

[503] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2581-728 (1998) (codified at 15 U.S.C. §§ 6501-6506).

[504] The use of the term "security" (traditionally defined as the preservation of confidentiality, integrity, and availability) seems confusing. Given COPPA's emphasis on privacy which, under U.S. law, is typically only concerned with confidentiality and, to some extent, integrity (*cf. supra* chapter 2.2.1), the enumeration of the

information"[505] collected from children under the age of 13.[506] These regulations are only to cover operators of a website or an online service operated for commercial purposes[507] if the website or service is directed to children or if the operator has "actual knowledge" that the website or service is collecting personal information from a child.[508] According to the COPPA Rule[509] promulgated by the FTC in 1999, the following are "appropriate measures to take:" using "secure web servers" and firewalls; deleting personal information once it is no longer being used; limiting employee access to data and providing those employees with data-handling training; and carefully screening the third parties to whom such information is disclosed.[510]

terms "confidentiality, security, and integrity" must be interpreted as indeed only referring to information confidentiality and integrity but not availability.

[505] *See* 15 U.S.C. § 6501(8) (2010) (defining "personal information" as "individually identifiable information about an individual collected online […]").

[506] 15 U.S.C. § 6502(b)(1)(D). *See* 15 U.S.C. § 6501(1) (defining "child" as "an individual under the age of 13"). This age-based bright-line approach has been criticized as demonstrating a suboptimal understanding of the drivers of child development. *See* Diana T. Slaughter-Defoe & Zhenlin Wang, *Information Security of Children's Data, in* HARBORING DATA: INFORMATION SECURITY LAW AND THE CORPORATION 145, 147 (Andrea M. Matwyshyn ed., 2009).

[507] *See* 15 U.S.C. § 6501(2) (defining "operator" as "any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated *for commercial purposes* […]" (emphasis added)).

[508] *See* 15 U.S.C. § 6502(b)(1)(D) (referring to "an operator of such a website or online service" and therefore implicitly to the wording of § 6502(b)(1)(A)).

[509] Children's Online Privacy Protection Rule; Final Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. pt. 312).

[510] *Id.* at 59,906. In light of the technological advances of the last years and the changed threat landscape, it is questionable whether these measures can still be considered "reasonable" under 15 U.S.C. § 6502(b)(1)(D).

For violations of the COPPA Rule, the FTC may bring enforcement actions under § 5 of the FTC Act.[511] State attorneys general may also enforce the COPPA Rule by filing *parens patriae* actions in federal court.[512]

4.1.5. The Communications Act

Section 222[513] of the Communications Act of 1934[514] establishes a duty for telecommunications carriers to protect the confidentiality of customer proprietary network information (CPNI).[515] This duty was further refined by the CPNI Regulations[516] adopted by the Federal Communications Commission (FCC) pursuant to § 222.

The personal scope of application of the CPNI Regulations is limited to telecommunications carriers (often simply referred to as carriers)[517] which are defined as any provider of "telecommunications services," excluding aggregators of such services.[518]

[511] *See* 15 U.S.C. § 6502(c) (providing that the regulations promulgated by the FTC shall be treated as a rule issued under 15 U.S.C. 57a (a)(1)(B)). *Cf. also* ANDREW FRACKMAN ET AL., INTERNET AND ONLINE PRIVACY: LEGAL AND BUSINESS GUIDE 62 (2002).

[512] 15 U.S.C. § 6504(a)(1) (providing that "[i]n any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the Commission prescribed under [15 U.S.C. § 6502(b)], the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—(A) enjoin that practice; (B) enforce compliance with the regulation; (C) obtain damage, restitution, or other compensation on behalf of residents of the State; or (D) obtain such other relief as the court may consider to be appropriate.").

[513] 47 U.S.C. § 222 (2010). This section was added to the Communications Act by Telecommunications Act of 1996 § 702, Pub. L. No. 104-104, 110 Stat. 56, 148-49 (1996).

[514] Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified as amended at 47 U.S.C. § 151 et seq.).

[515] *Cf. generally* Gina Marie Stevens & Tara Alexandra Rainson, *Data Security: Protecting the Privacy of Phone Records*, 887 PLI/PAT 337, 347 (2006).

[516] 47 C.F.R. §§ 64.2001-11 (2010). These rules were significantly amended in 2007 by Customer Proprietary Network Information; Final Rule, 72 Fed. Reg. 31,948 (June 8, 2007).

[517] *Cf. supra* chapter 2.3.1 (discussing communications services from a technical perspective).

[518] *See* 47 C.F.R. § 64.2003(o) (2010) (referring to Communications Act § 3(44), as amended, 47 U.S.C. 153(44)).

"Telecommunications services" are in turn defined as any "offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used."[519]

The material scope of application is limited to customer proprietary network information (CPNI) which generally encompasses information that relates to the use of a telecommunications service as well as information contained in phone bills.[520]

Under the FCC's CPNI Regulations, carriers have to implement certain safeguards to address the risk of unauthorized disclosure[521] as well as the risk of unauthorized use by the carrier itself.[522] However, since the latter is not an issue of information security, it will not be discussed here.[523]

Carriers have to implement "reasonable measures" not only to prevent but also to discover "attempts to gain unauthorized access to CPNI."[524] This requirement was introduced in response to a lively public debate[525] about a form of social engineering referred to as

[519] 47 U.S.C. § 153(44) (2010).

[520] See 47 C.F.R. § 64.2003(g) which refers to 47 U.S.C. § 222(h)(1) (defining CPNI as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information").

[521] *See* 47 C.F.R. § 64.2010 (2010).

[522] *See* 47 C.FR. § 64.2009 (2010).

[523] *Cf.* chapter 2.2.1 (discussing the distinction between data protection and information security).

[524] *See* 47 C.F.R. § 64.2010(a). *Cf. generally* Rosalind K. Allen, *Tough New FCC Rules on Customer Call Records*, COMM. LAW., Spring 2007, at 32.

[525] This debate was triggered by Hewlett-Packard's revelation in 2006 that it had hired private investigators who engaged in "pretexting" to obtain the phone records of its own board members and several journalists in order to identify the source of an information leak. *See* David A. Kaplan, *Suspicions and Spies in Silicon Valley*, NEWSWEEK, Sept. 18, 2006, *available at* http://www.newsweek.com/2006/09/17/suspicions-and-spies-in-silicon-valley.html. *Cf. also Hewlett-Packard's Pretexting Scandal: Hearing Before the Subcomm. on Oversight and*

"pretexting."[526] Accordingly, it primarily focuses on the proper authentication of customers prior to disclosing any CPNI[527] by prescribing certain authentication procedures that have to be followed with regard to all customers, except business customers.[528]

To authenticate a customer over the telephone, a carrier has to prompt the customer for a password or call him back at the telephone number of record.[529] When accessing CPNI online, customers have to be authenticated by a password.[530] When a customer seeks access to his CPNI at the carrier's retail location, he has to present a valid photo ID that matches the customer's account information.[531] Lastly, sending CPNI to the customer's address of record also fulfills the authentication requirements.[532]

With regard to the passwords that are used for authentication, the CPNI Regulations require that they are not prompted by the carrier asking for readily available biographical information

Investigations of the H. Comm. on Energy and Commerce, 109th Cong. 44-76 (2006) (statement of Patricia C. Dunn, Former Chairwoman of the Board, Hewlett-Packard Company).

[526] The FCC defines pretexting as "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records." *See* Report and Order and Further Notice of Proposed Rulemaking, Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Information; IP-Enabled Services, 22 F.C.C.R. 6,927, 6,928 n.1 (2007).

[527] *Cf.* ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL, STATE AND INTERNATIONAL LAW § 14:22 et seq. (2009).

[528] 47 C.F.R. § 64.2010(g) provides a business customer exemption by allowing carriers to bind themselves contractually to authentication regimes other than those described in § 64.2010 if (1) the business customer has a dedicated account representative and (2) the contract specifically addresses the carriers' protection of CPNI.

[529] *See* 47 C.F.R. § 64.2010(b). Note that this does not constitute two-factor authentication but an alternative between two one-factor authentication methods.

[530] *See* 47 C.F.R. § 64.2010(c).

[531] *See* 47 C.F.R. § 64.2010(d).

[532] *See* 47 C.F.R. § 64.2010(b).

or account information.[533] To establish the password, a carrier must authenticate the customer but has to do so without the use of readily available biographical information or account information.[534] A carrier may also create a back-up customer authentication method as long as it is not based on readily available biographical information or account information.[535]

Lastly, to help customers detect unauthorized changes to authentication credentials, carriers have to notify their customers immediately whenever a password, customer response to a back-up means of authentication, online account, or address of record is created or changed.[536] The notification may be performed by voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.[537]

If a carrier willfully[538] or repeatedly[539] fails to comply with the CPNI Regulations, the FCC may issue a Notice of Apparent Liability for Forfeiture pursuant to § 503(b)[540] of the Communications Act. The provider will then have a reasonable period of time (usually 30 days) to show, in writing, why a forfeiture penalty should not be imposed or should be

[533] *See* 47 C.F.R. § 64.2010(b) and (c). Note that this only means that a carrier may not ask a customer to use biographical information or account information as a password. It does not require the carrier to actually verify that a customer did not choose such a weak password on his own.

[534] *See* 47 C.F.R. § 64.2010(e).

[535] *See id.*

[536] *See* 47 C.F.R. § 64.2010(f).

[537] *See id.*

[538] *See* Communications Act of 1934 § 312(f)(1), 47 U.S.C. 312(f)(1) (defining "willful" as "the conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate").

[539] *See* Communications Act of 1934 § 312(f)(2), 47 U.S.C. 312(f)(2) (defining "repeated" as "the commission or omission of [any] act more than once or, if such commission or omission is continuous, for more than one day").

[540] 47 U.S.C. § 503(b).

reduced, or to pay the forfeiture.[541] If the proposed forfeiture penalty is not paid in full in response to the notice of apparent liability, the FCC will issue an order canceling or reducing the proposed forfeiture or requiring that it be paid in full.[542] If the forfeiture is not paid, the case will be referred to the Department of Justice which has to enforce the forfeiture order by bringing a civil suit against the provider.[543]

4.1.6. The Federal Trade Commission Act

Federal Trade Commission Act (FTC Act)[544] § 5(a)[545] directs the Federal Trade Commission (FTC) to prevent any person, partnership, or corporation[546] from using "unfair or deceptive acts or practices" in or affecting commerce or involving foreign commerce.[547] While the prohibition of deceptive acts or practices addresses issues with regard to transparency of security,[548] the FTC has used the prohibition of unfair acts or practices to effectively mandate the implementation of "reasonable" security controls.

[541] *See* 47 C.F.R. § 1.80(f)(3).

[542] *See* 47 C.F.R. § 1.80(f)(4).

[543] *See* Communications Act of 1934 § 504(a), 47 U.S.C. § 504(a). *See also* 47 C.F.R. § 1.80(f)(5).

[544] Federal Trade Commission Act of 1914, Pub. L. No. 63-203, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. §§ 41-58 (2010)).

[545] 15 U.S.C. § 45 (2010).

[546] Banks, savings and loan institutions, federal credit unions, common air carriers, and certain entities covered by the Packers and Stockyards Act of 1921, 7 U.S.C. § 181 et seq. are generally not covered by FTC Act § 5. *See* 15 U.S.C. § 45(a)(2).

[547] The Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 (US SAFE WEB Act), Pub. Law. No. 109-455, § 3, 120 Stat. 3372, 3372 (codified at 15 U.S.C. § 45 (a)(4)(A)) expanded the definition of "unfair or deceptive acts or practices" to include acts or practices involving foreign commerce that (1) cause or are likely to cause reasonably foreseeable injury within the United States"; or (2) "involve material conduct occurring within the United States."

[548] These are discussed *infra* in chapter 6.4.1.

Since 2005[549] the FTC has brought nine actions[550] against personal information controllers alleging that a "failure to take reasonable security measures to protect sensitive customer data" constitutes an unfair practice in violation of FTC Act § 5.[551] Unlike in the actions for deceptive acts or practices discussed *infra* in chapter 6.4.1, it is not relevant whether the act or practice was in violation of the company's public security claims.[552]

To bring an action for failure to implement reasonable security controls, the FTC relies on FTC Act § 5(n) which defines an act or practice to be "unfair" if (1) it "causes or is likely to cause substantial injury to consumers"; (2) such injury "is not reasonably avoidable by consumers themselves"; and (3) such injury is "not outweighed by countervailing benefits to consumers or to competition."[553]

The first element of "substantial consumer injury" is the "primary focus"[554] of the unfairness analysis. Significantly, the FTC considers as "injury" *inter alia*: (1) impersonation fraud;[555]

[549] The first such action was BJ's Wholesale Club, Inc., FTC File No. 0423160 (June 16, 2005).

[550] *Id.*; U.S. v. Choicepoint Inc., 1 06-CV-0198 (N.D. Ga. 2006) (stipulated final judgment); Cardsystems Solutions, Inc., FTC File No. 0523148 (Feb. 23, 2006); DSW Inc., FTC Docket No. C-4157 (Mar. 14, 2006); Reed Elsevier Inc., FTC File No. 0523094 (Mar. 27, 2008); The TJX Companies, Inc., FTC File No. 072-3055 (Mar. 27, 2008); CVS Caremark Corp., FTC Docket No. C-4259 (Feb. 18, 2009); Dave & Buster's, Inc., FTC File No. 0823153 (Mar. 25, 2010); Rite Aid Corp., FTC File No. 072-3121 (July 27, 2010). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[551] *See* Deborah Platt Majoras, Chairman, Fed. Trade Comm'n, Remarks at the Progress and Freedom Foundation Securing the Internet Project Internet Security Summit 6 (May 10, 2006), *available at* http://www.ftc.gov/speeches/majoras/060510ProgressFreedomFoundationRev051006.

[552] For example, BJ's Wholesale Club did not have a privacy policy in place and was not alleged to have acted in contradiction of any public statements made about the security of customers' personal information. *See* BJ's Wholesale Club, Inc., Complaint, FTC File No. 0423160 (2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf.

[553] FTC Act § 5(n), 15 U.S.C. § 45(n).

[554] Deborah Platt Majoras, Chairman, Fed. Trade Comm'n, Remarks at the Progress and Freedom Foundation Securing the Internet Project Internet Security Summit 8 (May 10, 2006), *available at* http://www.ftc.gov/speeches/majoras/060510ProgressFreedomFoundationRev051006.

(2) out-of-pocket expenses;[556] and (3) inconveniences to consumers such as having to obtain new personal ID numbers (e.g. new drivers' licenses)[557] or being unable to use one's credit card due to cancellation by the card issuer after the credit card data has been breached.[558]

The second element, requiring that the injury was not "reasonably avoidable by consumers themselves," is typically not an issue in the FTC's enforcement actions because consumer typically (1) could not have known that their personal information would be particularly vulnerable once given to the company in question; (2) could not have mitigated the risks to the personal information stored by the company; and (3) could not have done anything to prevent the resulting injury from occurring.[559]

The third element, requiring that the injury is "not outweighed by countervailing benefits," necessitates a cost-benefit analysis that compares the injury to the cost the company would have incurred to prevent it.[560] Recognizing that "breaches can happen […] even when a

[555] *See* U.S. v. Choicepoint Inc., 1 06-CV-0198 (N.D. Ga. 2006); Reed Elsevier Inc., FTC File No. 0523094 (Mar. 27, 2008); CVS Caremark Corp., FTC Docket No. C-4259 (Feb. 18, 2009); Rite Aid Corp., FTC File No. 072-3121 (July 27, 2010).

[556] *See* DSW Inc., FTC Docket No. C-4157 (Mar. 14, 2006) (customers had incurred out-of-pocket expenses such as the cost of ordering new checks).

[557] *See* The TJX Companies, Inc., FTC File No. 072-3055 (Mar. 27, 2008).

[558] *See* BJ's Wholesale Club, Inc., FTC File No. 0423160 (June 16, 2005); Cardsystems Solutions, Inc., FTC File No. 0523148 (Feb. 23, 2006). *Cf.* Deborah Platt Majoras, Chairman, Fed. Trade Comm'n, Remarks at the Progress and Freedom Foundation Securing the Internet Project Internet Security Summit 8 (May 10, 2006), *available at* http://www.ftc.gov/speeches/majoras/060510ProgressFreedomFoundationRev051006 (referring to "substantial injury in the form of inconvenience and time spent dealing with the blocking and re-issuance of their credit and debit cards" and further noting that such harms "are neither trivial nor speculative [but rather] real and substantial").

[559] *See id.* at 10.

[560] *Id.* at 9.

company has taken every reasonable precaution,"[561] the FTC aims to only initiate an enforcement action in cases in which the security breaches could have been prevented by "simple, readily available, low-cost measures."[562] However, the effect of this limitation may not be as significant as it might seem at first: In hindsight, most security breaches could have been prevented by inexpensive measures (e.g. installing a single patch on a single system). On the other hand, not knowing beforehand which vulnerability might be exploited, a company-wide security program has to be put in place to meaningfully mitigate risks. The implementation of such a security program is, however, always much more expensive than closing a single vulnerability.

Ultimately, the FTC does not provide companies with much guidance for what constitutes "reasonable" security, thereby creating significant amount of legal uncertainty.[563]

As regards the sanctions available for unfair acts or practices, FTC Act § 5 provides that the FTC may issue—after serving a complaint and hearing the defendant—a cease and desist order[564] which the defendant may then request to be reviewed by a federal court of appeals.[565]

[561] *Protecting our Nation's Cyber Space: Educational Awareness for the Cyber Citizen: Hearing Before the Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census of the H. Comm. on Government Reform*, 108th Cong. 14, 19 (2004) (statement of the Federal Trade Commission).

[562] Deborah Platt Majoras, Chairman, Fed. Trade Comm'n, Remarks at the Progress and Freedom Foundation Securing the Internet Project Internet Security Summit 9 (May 10, 2006), *available at* http://www.ftc.gov/speeches/majoras/060510ProgressFreedomFoundationRev051006. For example in the case of BJ'S Wholesale Club, an unnecessary risk was created by storing personal information for up to 30 days—longer than needed for business purposes. The appropriate security measure (deleting the information earlier) would not have caused any additional costs. *Cf.* BJ's Wholesale Club, Inc., FTC File No. 0423160 (June 16, 2005).

[563] *Cf.* Janine S. Hiller et. al., *Due Diligence on the Run: Business Lessons Derived from FTC Actions to Enforce Core Security Principles*, 45 IDAHO L. REV. 283, 309 (2009) (noting that the FTC "therefore leave[s] many of the hard decisions about necessary security to the individual business"); Travis D. Breaux & David L. Baumer, *Legally "Reasonable" Security Requirements: A 10-year FTC Retrospective*, COMPUTERS & SECURITY (forthcoming 2011) (noting that "the obligations [imposed by the FTC] fall short of explaining *how* companies can ensure that the steps they have taken are consistent with the full extent of these obligations" (emphasis in original)).

[564] FTC Act § 5(b), 15 U.S.C. § 45(b).

Any violation of FTC Act § 5 that is performed with "actual knowledge or knowledge fairly implied on the basis of objective circumstances [that the act or practice in question is prohibited]" is subject to a civil penalty of up to $10,000 for each violation.[566] Furthermore, violations of an order that has become final are subject to a civil penalty of the same amount.[567]

Remarkably, in the above-cited enforcement actions—all of which have been settled rather than fully litigated—the FTC has not sought any civil penalties for violation of FTC Act § 5.[568] However, the settlement agreements typically require measures nearly identical to those mandated by the FTC Safeguards Rule[569] to be implemented and maintained for twenty years.[570]

[565] FTC Act § 5(c), 15 U.S.C. § 45(c).

[566] *See* FTC Act § 5(m)(1)(A), 15 U.S.C. § 45(m)(1)(A). In the case of a continuing violation, each day of continuance is treated as a separate violation. FTC Act § 5(m)(1)(C), 15 U.S.C. § 45(m)(1)(C).

[567] *See* FTC Act § 5(l), 15 U.S.C. § 45(l).

[568] However, when other statutes such as HIPAA or FCRA had also been violated, the FTC did seek civil penalties under those statutes. See, for example, U.S. v. Choicepoint Inc., 1 06-CV-0198 (N.D. Ga. 2006) where Choicepoint agreed to pay $10 million in civil penalties and $5 million to redress consumers who became victims of impersonation fraud and Rite Aid Corp., FTC File No. 072-3121 (July 27, 2010) where Rite Aid agreed to pay $1 million to settle allegations of HIPAA violations. *Cf. also* Joel B. Hanson, *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, 4 SHIDLER J. L. COM. & TECH. 11, 34-37 (2008).

[569] *See supra* chapter 4.1.2.1 (describing the requirements under the FTC Safeguards Rule).

[570] *See Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 27, 28 (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission) ("The consent orders […] have required the companies to implement appropriate information security programs that generally conform to the standards that the Commission set forth in the GLBA Safeguards Rule."). *Cf. also* Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, FED. LAW., Sept. 2007, at 39, *available at* 54-SEP Fed. Law. 39 (Westlaw) (criticizing the expansion of the personal scope of application of the FTC Safeguards Rule).

4.1.7. Safeguard Requirements under California and New York State Law

4.1.7.1. Safeguard Requirements for Social Security Numbers

As further discussed *infra* in chapter 4.1.10.1, for a person seeking to commit impersonation fraud, Social Security numbers (SSNs) are of more usefulness, than any other kind of personal information. In an attempt to make SSNs harder to obtain for unauthorized persons, the California legislator passed Senate Bill 168[571] in 2001 which became effective on July 1, 2002. As of February 2011, at least 37 other states have passed similar laws.[572]

Senate Bill 168 applies to any person or entity, not including a state or local agency. Besides mandating that SSNs shall generally be treated confidential (i.e. not made available to the public, printed on membership cards, or on mailings),[573] it establishes two security related requirements: (1) one must not require an individual to transmit his SSN over the Internet "unless the connection is secure or the Social Security number is encrypted";[574] and (2) one must not require an individual to use her SSN to access a website unless "a password or unique personal identification number or other authentication device is also required to access the Web site."[575]

[571] 2001 Cal. Legis. Serv. Ch. 720 (S.B. 168) (West) (codified at CAL. CIV. CODE §§ 1785, 1798.85 as amended).

[572] *See* http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/state-laws-social-security.html (last accessed Feb. 10, 2011).

[573] *See* CAL. CIV. CODE § 1798.85(a)(1), (2), and (5) (West 2010).

[574] CAL. CIV. CODE § 1798.85(a)(3).

[575] CAL. CIV. CODE § 1798.85(a)(4). *Cf.* Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 916 (N.D. Cal. 2009) (holding that requiring an individual to use his SSN to submit an online job application does not violate CAL. CIV. CODE § 1798.85(a)(4)).

Senate Bill 168 does not provide an enforcement mechanism itself. However, a violation of Senate Bill 168 constitutes an act of "unfair competition."[576] The attorney general may therefore bring an action for an injunction[577] or for civil penalties.[578] A private cause of action, that was independent of possible injuries suffered by the plaintiff, has been eliminated by Proposition 64[579] which was passed in 2004.[580] However, Proposition 64 did not eliminate competitor actions for injunctive relief.[581] The possibility to recover damages under Senate Bill 168 is discussed in chapter 5.1.5.1.

In 2006, New York adopted provisions identical to California Senate Bill 168.[582] These provisions are subject to the enforcement by the attorney general who may bring an action for an injunction and/or may seek civil penalties.[583]

[576] *Cf.* CAL. BUS. & PROF. CODE § 17200 (stating that "unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice […]").

[577] *See* CAL. BUS. & PROF. CODE § 17204.

[578] *See* CAL. BUS. & PROF. CODE § 17206.

[579] *See* 2004 Cal. Legis. Serv. Prop. 64 (West). CAL. BUS. & PROF. CODE § 17204 as amended by Proposition 64 provides that a person may only bring an action under CAL. BUS. & PROF. CODE § 17200 et seq. if she has actually "suffered injury in fact and has lost money or property as a result of the unfair competition." *See* Bivens v. Gallery Corp., 36 Cal. Rptr. 3d 541, 548 (2005), *reh'g denied*, 2005 Cal. App. LEXIS 2037 (Cal. Ct. App. 2006), *review granted*, *depublished*, 130 P.3d 518 (Cal. 2006), *review dismissed*, 154 P.3d 1001 (Cal. 2007). *Cf.* Sharon J. Arkin, *The Unfair Competition Law after Proposition 64: Changing the Consumer Protection Landscape*, 32 W. ST. U. L. REV. 155 (2005); Jacquetta Lannan, *Saving 17200: An Analysis of Proposition 64*, 46 SANTA CLARA L. REV. 451 (2006); Christopher W. Arledge, *Standing Under the Unfair Competition Law is Unlikely to Exist for Competitors*, 50 ORANGE COUNTY LAW. 51 (2008).

[580] *Cf.* CAL. CONST. art. II, § 8 (stating that "[t]he initiative is the power of the electors to propose statutes and amendments to the Constitution and to adopt or reject them").

[581] *See* Clayworth v. Pfizer, Inc., 233 P.3d 1066, 1088 (Cal. 2010) (holding that the right to seek injunctive relief under CAL. BUS. & PROF. CODE § 17203 is not dependent on the right to seek restitution). *Cf. also* Finelite, Inc. v. Ledalite Architectural Prods., No. C-10-1276 MMC, 2010 WL 3385027 (N.D. Cal. Aug. 26, 2010) (applying *Clayworth*).

[582] *See* N.Y. GEN. BUS. LAW § 399-dd (McKinney 2010). N.Y. GEN. BUS. LAW § 399-dd(2)(f), which was enacted in 2008, goes beyond California S.B. 168 by also prohibiting the encoding or embedding of a Social Security number "in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the social security number as required by this section."

4.1.7.2. Disposal Requirements

Mandatory disposal safeguards were first introduced in California by Assembly Bill 2246[584] which was passed in 2000 and went into effect on January 1, 2001. California Civil Code § 1798.81 as amended in 2009 by Assembly Bill 1094[585] mandates that a business takes all reasonable steps to dispose, or arrange for the disposal, of customer[586] records within its custody or control containing "personal information" when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.[587] It has to be emphasized that "personal information" is defined very broadly as "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual" not including "publicly available information."[588]

A violation of California Civil Code § 1798.81 constitutes an act of unfair competition for which the attorney general may bring an action for an injunction[589] or may seek civil

[583] N.Y. GEN. BUS. LAW § 399-dd(7). An injunction does not require proof that any person has, in fact, been injured or damaged. *Id.* The court may impose a civil penalty of not more than $1000 for a single violation and not more than $100,000 for multiple violations resulting from a single act or incident. For a second violation the maximum penalties are increased to $5,000 and $250,000 respectively. *Id.*

[584] 2000 Cal. Adv. Legis. Serv. 5942 (Deering) (codified at CAL. CIV. CODE §§ 1798.80-82).

[585] 2009 Cal. Legis. Serv. Ch. 134 (West) (effective as of Jan. 1, 2010).

[586] *See* CAL. CIV. CODE §§ 1798.80(c) (West 2010) (defining "customer" as "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business").

[587] This wording indicates that only very strong encryption is sufficient.

[588] CAL. CIV. CODE § 1798.80(e).

[589] *See* CAL. BUS. & PROF. CODE § 17204.

penalties.[590] Individuals have no private right of action unless they have been injured (see chapter 5.1.4).[591]

In 2006, New York adopted a similar provision.[592] It prohibits any business from disposing of records containing "personal identifying information" unless the business or other person under contract with the business takes one of the following measures: (a) shredding the records; (b) destroying the personal identifying information contained in the records; (c) modifying the records to make the personal identifying information unreadable; or (d) taking actions "consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information."[593] These requirements are enforced by the attorney general who may seek an injunction[594] or civil penalties of not more than $5,000.[595]

It is worth pointing out two differences to California Civil Code § 1798.81. First, the term "personal identifying information," which determines the material scope of application, is defined rather narrowly as personal information consisting of any information in combination with: (i) a Social Security number; (ii) driver's license number or non-driver identification

[590] *See* CAL. BUS. & PROF. CODE § 17206.

[591] CAL. CIV. CODE § 1798.84(e) provides that any business that violates, proposes to violate, or has violated, *inter alia,* § 1798.81 may be enjoined. However, the legislative history clearly indicates that only customers injured by a violation have standing. 2000 Cal. Adv. Legis. Serv. 5942 (Deering) (stating that "[a]ny customer injured by a business' violation of these provisions would be entitled to institute a civil action to recover damages, obtain injunctive relief, or seek other remedies.").

[592] *See* 2006 N.Y. Sess. Laws Ch. 65 (codified as amended at N.Y. GEN. BUS. LAW § 399-h) (effective as of Dec. 4, 2006).

[593] N.Y. GEN. BUS. LAW § 399-h (McKinney 2010).

[594] Proof that any person has, in fact, been injured or damaged by the violation is not required. N.Y. GEN. BUS. LAW § 399-h(3).

[595] N.Y. GEN. BUS. LAW § 399-h(3). Acts arising out of the same incident or occurrence constitute a single violation. *Id.*

card number; or (iii) mother's maiden name, a number or code for a financial service, savings account, checking account, debit card, ATM, or an electronic serial number or personal identification number.[596] Second, New York General Business Law § 399-h is more flexible than California Civil Code § 1798.81 in the sense that measures that are consistent with commonly accepted industry practices are deemed sufficient—if the business "reasonably believes" in the effectiveness of the measure.

4.1.7.3. General Safeguard Requirements under California Assembly Bill 1950

Assembly Bill 1950[597] was passed in 2004 and became effective on January 1, 2005. It requires businesses that "own or license"[598] personal information about a California resident to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[599] While New York has not yet adopted a similar law, at least nine states have done so.[600]

Assembly Bill 1950's personal scope of application covers businesses, whether or not they are operated for a profit,[601] but excludes entities subject to[602]: the California Confidentiality of

[596] N.Y. Gen. Bus. Law § 399-h(1)(d).

[597] 2004 Cal. Adv. Legis. Serv. 381 (codified at CAL. CIV. CODE § 1798.81.5 (West 2010))

[598] *See* CAL. CIV. CODE § 1798.81.5(a) (stating that the phrase "owns or licenses" includes, but is not limited to, "personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates").

[599] CAL. CIV. CODE § 1798.81.5(b).

[600] *See* ARK. CODE ANN. § 4-110-104(b) (West 2010); CONN. GEN. STAT. ANN. § 42-471(a) (West 2010); MD. CODE ANNN., COM. LAW § 14-3503 (West 2010); MASS. GEN. LAWS. ANN. ch. 93H, § 2(a) (West 2010); NEV. REV. STAT. ANN. § 603A.210 (West 2010); OR. REV. STAT. ANN. § 646A.622 (West 2010); R.I. GEN. LAWS. § 11-49.2-2(2) and (3) (2010); TEX. BUS. & COM. CODE ANN. § 521.052(a) (Vernon 2010); and UTAH CODE ANN. § 13-44-201(1)(a) (West 2010). *Cf.* AM. BAR ASS'N, DATA SECURITY HANDBOOK 50 (2008).

[601] *See* CAL. CIV. CODE § 1798.80(a).

Medical Information Act;[603] the California Financial Information Privacy Act;[604] the HIPAA Security Rule;[605] or the confidentiality requirements of the California Vehicle Code with respect to DMV records.[606] Furthermore, businesses that are regulated by state or federal law providing greater protection to personal information than that provided by Assembly Bill 1950 are deemed in compliance if they comply with that state or federal law.[607]

The material scope of application covers "personal information" about California residents,[608] which is defined as an individual's name[609] in combination with: (a) her Social Security number; (b) her driver's license number or California identification card number; (c) her account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (d) medical information.[610] The material scope if further narrowed by excluding information that is lawfully made available to the general public from federal, state, or local government

[602] *See* CAL. CIV. CODE § 1798.81.5(e)(1)-(4).

[603] Confidentiality of Medical Information Act, CAL. CIV. CODE § 56 et seq. (West 2010). CA. CIV. CODE § 56.20(a) provides that employers who receive medical information have to establish "appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information." It therefore employs the same standard as A.B. 1950.

[604] California Financial Information Privacy Act, CAL. FIN. CODE § 4050 et seq. (West 2010). As it does not provide specific obligations with regard to security safeguards, it will not be discussed here.

[605] *See* chapter 4.1.1.

[606] *See* CAL. VEH. CODE § 1808.47 (West 2010) (stating that any person who has access to confidential or restricted information from the Department of Motor Vehicles shall establish "procedures to protect the confidentiality of those records," thereby establishing a similar standard as A.B. 1950).

[607] CAL. CIV. CODE § 1798.81.5(e)(5).

[608] Even businesses that do not have an establishment in California may therefore be affected by A.B. 1950. *Cf.* Tyler Paetkau & Roxanne Torabian-Bashardoust, *California Deals with ID Theft: The Promise and the Problems*, BUS. L. TODAY, May-June 2004, at 37, 37 (describing this effect with regard to CAL. CIV. CODE § 1798.82).

[609] First name or first initial in combination with the last name. CAL. CIV. CODE § 1798.81.5(d)(1).

[610] CAL. CIV. CODE § 1798.81.5(d)(1)(A)-(D). "Medical information" is defined as "individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional." CAL. CIV. CODE § 1798.81.5(d)(2).

records.[611] Moreover, Assembly Bill 1950 also does not apply if the personal information is "encrypted."[612]

Assembly Bill 1950 mandates the implementation and maintenance of "reasonable security procedures and practices" to protect from losses of confidentiality (due to "unauthorized access" or "disclosure"), permanent losses of availability (due to "destruction"), or losses of integrity (due to "modification").[613] These procedures and practices have to be "appropriate to the nature of the information."[614] Since Assembly Bill 1950 does not further define the standard of "reasonableness" or "appropriateness", it has been criticized for being too vague.[615]

Furthermore, if personal information about a California resident is disclosed pursuant to a contract with a nonaffiliated third party, the business must require by contract that the third party implement and maintain "reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[616]

[611] CAL. CIV. CODE § 1798.81.5(d)(3). The exclusion of information based on a lack of confidentiality interest is somewhat inconsistent as A.B. 1950 does not only protect the confidentiality but also the integrity and availability of information.

[612] CAL. CIV. CODE § 1798.81.5(d)(1). It has to be noted that the statute does not provide any indication as to the required strength of the encryption.

[613] CAL. CIV. CODE § 1798.81.5(b).

[614] *Id.*

[615] *See, e.g.,* Anthony D. Milewski Jr., *Compliance with California Privacy Laws: Federal Law also Provides Guidance to Businesses Nationwide*, 2 SHIDLER J. L. COM. & TECH. 19 (2006); Chad Pinson, *New Legal Frontier: Mass Information Loss and Security Breach*, 11 SMU SCI. & TECH. L. REV. 27, 38 (2007).

[616] CAL. CIV. CODE § 1798.81.5(c). It has to be noted that the statute does not expressly require any oversight of the third party.

A violation of Assembly Bill 1950 constitutes an act of unfair competition[617] for which the attorney general may bring an action for an injunction[618] or seek civil penalties.[619] A private right of action is neither provided under Assembly Bill 1950[620] nor under unfair competition law,[621] unless the individual has been injured (see chapter 5.1.4).

4.1.7.4. Security Freeze of Credit Reports

A security freeze of a credit report can be generally described as a mechanism that allows a consumer to control when a consumer reporting agency may release the consumer's credit report. As of February, 2011, at least 47 states—including California and New York—as well as the District of Columbia have enacted security freeze laws.[622]

On its face, such a measure rather falls in the policy area of data protection than information security.[623] However, it has an important side-effect that warrants a brief discussion here: security freeze laws do not only limit the circulation of consumer reports but also serve as a type of authentication mechanism in order to prevent "identity theft" and, by extension, the

[617] *See* CAL. BUS. & PROF. CODE § 17200 (West 2010) (stating that "unfair competition" shall include "any unlawful […] business act or practice").

[618] *See* CAL. BUS. & PROF. CODE § 17204.

[619] *See* CAL. BUS. & PROF. CODE § 17206.

[620] CAL. CIV. CODE § 1798.84(e) provides that any business that violates, proposes to violate, or has violated, *inter alia,* § 1798.81 may be enjoined. However, the legislative history clearly indicates that only customers injured by a violation have standing. 2000 Cal. Adv. Legis. Serv. 5942 (Deering) (stating that "[a]ny customer injured by a business' violation of these provisions would be entitled to institute a civil action to recover damages, obtain injunctive relief, or seek other remedies.").

[621] CAL. BUS. & PROF. CODE § 17204 as amended by Proposition 64 provides that a person may *only* bring an action under CAL. BUS. & PROF. CODE § 17200 et seq. if she has actually "suffered injury […] and has lost money or property as a result of the unfair competition." *See supra* chapter 4.1.7.1.

[622] *See* http://www.ncsl.org/default.aspx?tabid=12475 (last accessed Feb. 10, 2011). For a survey of the different security freeze state laws see, for example, TARA ALEXANDRA RAINSON, CONG. RESEARCH SERV., IDENTITY THEFT LAWS: STATE PENALTIES AND REMEDIES AND PENDING FEDERAL BILLS, CRS REPORT FOR CONGRESS RL34028, at 4 (2007), *available at* http://opencrs.com/document/RL34028/2007-08-06/download/1005/.

[623] *See* chapter 2.2.1 (discussing the distinction between data protection and information security).

compromise of the integrity of a consumer's credit history.[624] The rationale is that most companies will attempt to obtain a consumer's credit report before extending credit to him. If, however, the credit report cannot be obtained due to a security freeze, it will not be possible to commit "identity theft."[625] However, it has to be stressed that a security freeze does not prohibit additions and/or changes to a consumer's credit history.

Under both California and New York law, a consumer may place a "security freeze"[626] on his credit history[627] and may subsequently lift it temporarily for a period of time or for a specific party[628] (typically for an entity from which the consumer wants to obtain credit and therefore expects to seek his credit report). In order to allow consumers to authenticate themselves for the purpose of temporarily lifting or removing a previously requested security freeze, a consumer reporting agency has to provide consumers with a "unique personal identification number or password" when first placing the security freeze on a consumer's credit report.[629] In California and New York, a security freeze does not have an absolute effect. Both states provide certain exemptions such as for entities with which the consumer has had an account

[624] *See* THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT—A STRATEGIC PLAN 46 (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

[625] *Cf.* Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports To Prevent Lending to Impostors, in* SECURING PRIVACY IN THE INTERNET AGE 207, 214 et seq. (Anupam Chander et al. eds., 2008) (arguing that credit freeze would put impersonation fraud "on ice" if credit reports were freezed by default).

[626] CAL. CIV. CODE § 1785.11.2(a) (West 2010) (defining "security freeze" as "a notice placed in a consumer's credit report, at the request of the consumer, and subject to certain exceptions, that prohibits the consumer credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer"); N.Y. GEN. BUS. LAW § 380-a(m) (McKinney 2010) (defining "security freeze" as "a notice placed in the consumer credit report of or relating to a consumer, at the request of such consumer and subject to certain exceptions, that prohibits the consumer credit reporting agency from releasing the consumer credit report, the contents of such report or the credit score of such consumer"). With regard to CAL. CIV. CODE § 1785.11.2, compare generally LESLIE M. LARSEN ET AL., 13A CALIFORNIA JURISPRUDENCE 3D § 489 (2010).

[627] *See* CAL. CIV. CODE § 1785.11.2(a); N.Y. GEN. BUS. LAW § 380-t(a).

[628] *See* CAL. CIV. CODE § 1785.11.2(d); N.Y. GEN. BUS. LAW § 380-t(d).

[629] *See* CAL. CIV. CODE § 1785.11.2(c); N.Y. GEN. BUS. LAW § 380-t(c).

or contract[630] or, under California law, with regard to lawfully obtained public record information.[631]

It should be stressed that a security freeze has to be requested individually from each national consumer reporting agency (TransUnion, Equifax, and Experian). Under California law, a consumer reporting agency may charge for a security freeze, its removal, or its temporary lift up to $10 ($5 in the case of seniors that are 65 years of age or older), except that "identity theft" victims may not be charged.[632] Under New York law, a consumer reporting agency may only charge $5, except that no charge may be made for "identity theft" victims as well as the first security freeze requested from a particular consumer reporting agency.[633]

4.1.8. The EU Data Protection Directive

The EU Data Protection Directive[634] (hereinafter *EUDPD*) which was transposed by all Member States[635] has a very broad scope of application. It applies to the "processing"[636] of all

[630] *See* CAL. CIV. CODE § 1785.11.2(l); N.Y. GEN. BUS. LAW § 380-t(m).

[631] *See* CAL. CIV. CODE § 1785.11.2(n). This subsection was introduced in 2007 by Assembly Bill 1298, 2007 Cal. Legis. Serv. Ch. 699 (West) which took into account U.D. Registry, Inc. v. State, 50 Cal. Rptr. 3d 647, 662 (Cal. Ct. App. 2006) (holding that the prohibition of "truthful reporting of lawfully available and obtained public record information" under § 1785.11.2 was an excessive restriction and thus was an unconstitutional violation of free speech rights as applied to credit reporting agencies). *Cf.* Patricia Covington & Meghan Musselman, *Privacy and Data Security Developments Affecting Consumer Finance in 2008*, 64 BUS. LAW. 533, 538 (2009).

[632] *See* CAL. CIV. CODE § 1785.11.2(m).

[633] *See* N.Y. GEN. BUS. LAW § 380-t(n).

[634] Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

[635] *Cf.* http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (last accessed Feb. 10, 2011).

[636] *See* EUDPD art. 2(b) (defining "processing" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"). *Cf. also* EUDPD Recital 27 (stating "as regards manual processing, this Directive covers only filing systems, not unstructured files").

"personal data"[637] except where (1) the processing occurs in the course of an activity "which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union";[638] or (2) the processing is performed by a natural person in the course of a purely personal or household activity.[639]

To refer to the entity on whose behalf personal data is processed, the EUDPD uses the term "controller."[640] If the processing is outsourced to another entity, that entity is referred to as a "processor."[641]

EUDPD article 17 specifically addresses the issue of security of processing. It mandates that Member States require controllers to implement "appropriate technical and organizational measures"[642] to protect personal data against "accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access,"[643] in particular where the processing

[637] *See* EUDPD art. 2(a) (defining "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity").

[638] Before the Lisbon Treaty went into force on Dec. 1, 2009, the EU's legal predecessor, the European Community, had no competence in the area of common foreign and security policy (Title V) and police and judicial cooperation in criminal matters (Title VI). *See* art. 1 of the Treaty on European Union as amended by the Lisbon Treaty (providing that "[t]he Union shall replace and succeed the European Community").

[639] EUDPD art. 3.

[640] *See* EUDPD art. 2(d) (defining "controller" as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law"). *Cf. supra* chapter 2.2.1 (defining the term "personal information controller" as used in this thesis).

[641] *See* EUDPD art. 2(e) (defining "processor" as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller").

[642] The fact that the EUDPD only refers to "technical" and "organizational" but not to "physical" measures has no limiting effect. *See Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security*, at 37, COM (90) 314 final (Sept. 13, 1990) (stating that technical measures include "safety measures for access to data processing and storage locations").

[643] Note that the EUDPD explicitly refers to accidents as well as unlawful acts. Also note that the acts of "destruction or […] loss, alteration, unauthorized disclosure or access" can be equated to a permanent loss of

involves the transmission of data over a network, and against all other unlawful forms of processing.[644] For the purpose of keeping proof, the requirements relating to these measures have to be in writing or in another equivalent form.[645]

With regard to what measures are to be considered "appropriate," the Directive states that the measures shall ensure "a level of security appropriate to the risks represented by the processing and the nature of the data to be protected," taking into account "the state of the art and the cost of [the measures'] implementation."[646]

If the controller decides to outsource the data processing, he must "choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out."[647] Furthermore, the controller must "ensure compliance with those measures."[648] The relationship between the controller and the processor must also be governed by a written[649] contract or legal act

availability, a loss of integrity, and a loss of confidentiality. *Cf. also* art. 7 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, Council of Europe CETS No. 108, 1496 U.N.T.S. 66 (stating that "[a]ppropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination").

[644] EUDPD art. 17(1). All national laws adopted by the Member States pursuant to art. 17 state, in only slightly varying terms, that "appropriate technical and organisational measures" must be implemented. *See* DOUWE KORFF, STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE – COMPARATIVE SUMMARY OF NATIONAL LAWS 157 (2002), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf.

[645] EUDPD art. 17(4).

[646] EUDPD art. 17(1) sentence 2. *Cf.* ULRICH DAMMANN & SPIROS SIMITIS, EG-DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE], art. 17 cmt. 6 (1997) (stating that what is "appropriate" would have to be determined by the magnitude of the risks to which the data subjects' rights are exposed, in particular by the probability of any damages).

[647] EUDPD art. 17(2).

[648] *Id.*

[649] *See* EUDPD art. 17(4) (stating that "[f]or the purposes of keeping proof, the parts of the contract or the legal act relating to data protection […] shall be in writing or in another equivalent form.").

binding the processor to the controller and stipulating in particular that: (1) "the processor shall act only on instructions from the controller"; and (2) "the obligations [with regard to the security of processing], as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor."

National law adopted by Member States pursuant to the EUDPD is subject to the enforcement by national supervisory authorities[650] which have to "act with complete independence in exercising the functions entrusted to them."[651] Pursuant to article 24, Member States have to adopt "suitable measures to ensure the full implementation" of the EUDPD. In particular, they have to provide sanctions to be imposed in case of infringement of the provisions adopted pursuant to the EUDPD.[652]

4.1.9. The EU ePrivacy Directive

Parliament and Council Directive 2002/58[653] (hereinafter *ePrivacy Directive*) translates the principles set out in the EUDPD into specific rules for the telecommunications sector.[654] The

[650] *See* EUDPD art. 28(1) (stating that "[e]ach Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive."). The EUDPD does not obligate the Member States to create a private cause of action against controllers who do not implement adequate security measures. EUDPD art. 22 states that "Member States shall provide for the right of every person to a judicial remedy for any *breach of the rights* guaranteed him by the national law applicable to the processing in question" (emphasis added). However, under the EUDPD, data subjects do not have a "right to adequate security measures" (for the data subjects' rights see art. 12-15).

[651] EUDPD art. 28(1). *Cf.* Case C-518/07, Comm'n v. Germany, 2010 ECJ EUR-Lex LEXIS 524 (Mar. 9, 2010) (holding that the requirement of "complete independence" is not fulfilled if supervisory authorities are subjected to State scrutiny as it is the case in the Germany *Länder*). *Cf. also* art. 1(3) of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Nov. 8, 2001, Council of Europe CETS No. 181, 2297 U.N.T.S. 195 (requiring that "[t]he supervisory authorities shall exercise their functions in complete independence").

[652] *See* EUDPD art. 24.

[653] 2002 O.J. (L 201) 37 (EC) as amended.

[654] *See* ePrivacy Directive recital 4. *Cf. also* ePrivacy Directive art. 1 (stating with regard to the ePrivacy Directive's scope and aim that the Directive "harmonises the provisions of the Member States required to ensure

Directive's security requirements which are stipulated in article 4 are therefore limited to "provider[s] of a publicly available electronic communications service."[655]

Since the ePrivacy Directive does not define this term, the definitions of Parliament and Council Directive 2002/21[656] (hereinafter *Telecoms Framework Directive*) have to be applied.[657] Providers of "publicly available electronic communications services" have to be distinguished from providers of "public communications networks." The term "public communications network" is defined in Telecoms Framework Directive article 2(d) as "an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services."[658] Accordingly, providers of "communications networks" only provide the physical network infrastructure that is needed by providers of "electronic communications services" to provide their services.[659]

Article 2(c) of the Telecoms Framework Directive defines an "electronic communications service" as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks."[660] This includes "telecommunications services and transmission services in networks used for broadcasting"

an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.").

[655] *See* ePrivacy Directive art. 4(1). *Cf. id.* art. 3(1) (defining the Directive's general scope more broadly so as to also include "public communications networks supporting data collection and identification devices").

[656] 2002 O.J. (L 108) 33 (EC).

[657] *See* ePrivacy Directive art. 2 (stating that "save as otherwise provided, the definitions in […] Directive 2002/21/EC […] shall apply").

[658] Telecoms Framework Directive art. 2(d).

[659] *See* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 44 (2010) (F.R.G.).

[660] Telecoms Framework Directive art. 2(c).

but excludes services "providing, or exercising editorial control over, content."[661] This exclusion makes clear that content providers are not providers of "electronic communications services."[662]

The key requirement that further distinguishes "electronic communications services" from online services[663] is that the former has to consist "mainly in the *conveyance of signals* on electronic communications networks."[664] In this regard, the conveyance of signals must not be confused with the initiation of such a conveyance.[665] This point is well illustrated by an example from the physical world: A person mailing a letter from New York City to someone in San Francisco does not perform the "conveyance" of the letter himself; he or she merely initiates the conveyance which is indeed performed by the U.S. Postal Service (the communications service provider, so to speak).[666]

Similarly, hosting providers or e-mail service providers do not convey signals themselves. They only initiate such a conveyance (and receive signals conveyed to them) by relying on Internet access providers and Internet backbone providers which—very much like the U.S. Postal Service—perform the actual conveyance of the signals.

[661] *Id.*

[662] *Cf.* Telecoms Framework Directive recital 10 (stating that "services […] such as the provision of web-based content" are not electronic communications services). *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 44 (2010) (F.R.G.)

[663] *See supra* chapter 2.3.2 (describing online services).

[664] Telecoms Framework Directive art. 2(c) (emphasis added). The definition of the term "electronic communications network" in Telecoms Framework Directive art. 2(a) covers circuit-switched networks (e.g. the plain old telephone service) as well as packet-switched networks (e.g. the Internet). *Cf. supra* chapter 2.3.1 (discussing the architecture of the Internet).

[665] *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 44 (2010) (F.R.G.) (emphasizing this distinction).

[666] *See id.*

In the terms of the TCP/IP networking model, the conveyance of signals is a function of the link layer and, to some extent, of the network layer.[667] Accordingly, from a technical perspective, "electronic communications services" can be understood as services that are provided on the first two layers of the TCP/IP networking model.

In summary, the scope of application of ePrivacy Directive article 4 covers telephone and Internet access providers as well as Internet backbone providers,[668] assuming that they do not only provide the necessary physical network infrastructure (i.e. only act as a provider of a "public communications network") but also provide the electronic communications service themselves.[669]

Article 4(1) rephrases the requirements under EUDPD article 17 by stating that a provider of a publicly available electronic communications service must take "appropriate technical and organizational measures to safeguard security of its services." Security, in this context, is appraised in the light of EUDPD article 17.[670] Consequently, if the communications service provider (who is to be considered the controller as defined in the EUDPD) relies on a "provider of a public communications network" to provide his service, he must take the appropriate security measures "in conjunction with" the provider of the communications network.[671]

[667] *Cf. supra* chapter 2.3.2 (describing the TCP/IP networking model).

[668] *Cf. supra* chapter 2.3.1 (describing both Internet access providers and Internet backbone provider from a technical perspective).

[669] *See* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 44 (2010) (F.R.G.).

[670] *See* ePrivacy Directive Recital 20 last sentence.

[671] ePrivacy Directive art. 4(1).

Much like the EUDPD, the ePrivacy Directive states with regard to what measures are to be considered "appropriate," that "these measures shall ensure a level of security appropriate to the risk presented," having regard to "the state of the art and the cost of their implementation."[672]

Parliament and Council Directive 2009/136[673] (hereinafter *Citizens' Rights Directive* or *CRD*) which was adopted in December 2009 as part of the "Telecoms Package"[674] and has to be transposed by May 25, 2011[675] amended ePrivacy Directive article 4 to provide certain minimum requirements. Article 4(1a) of the ePrivacy Directive as amended by the CRD provides that the measures referred to under article 4(1) shall at least include a form of access control[676] and the implementation of a security policy[677] with respect to the processing of personal data.[678] These requirements are rather vague. A provision that would have granted the Commission the power to adopt "technical implementing measures"[679] was successfully opposed by the Council[680] and the European Parliament.[681]

[672] *Id.*

[673] Parliament and Council Directive 2009/136, 2009 O.J. (L 337) 11 (EC).

[674] This legislative package consists of three legal acts: the Citizens' Rights Directive, Parliament and Council Directive 2009/140, 2009 O.J. (L 337) 37 (EC) (discussed partly *supra* in chapter 4.3.1 and *infra* in chapter 6.3.2), and Parliament and Council Regulation 1211/2009, 2009 O.J. (L 337) 1 (EC).

[675] CRD art. 4.

[676] *See* ePrivacy Directive art. 4(1a) first indent (stating that it has to be ensured "that personal data can be accessed only by authorised personnel for legally authorised purposes"). *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.1 (2009) (defining "access control" as "means to ensure that access to assets is authorized and restricted based on business and security requirements").

[677] *Cf.* CRD Recital 57 (stating that the security policy "should be established in order to identify vulnerabilities in the system, and monitoring and preventive, corrective and mitigating action should be regularly carried out").

[678] *See* ePrivacy Directive art. 4(1a) third indent. Note that the second indent of ePrivacy Directive art. 4(1a) only rephrases the general requirements of ePrivacy Directive art. 4(1a) read in conjunction with EUDPD art. 17(1).

[679] *See Commission Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive*

Pursuant to ePrivacy Directive article 15a, Member States have to lay down rules on penalties applicable to infringements of the national provisions adopted pursuant to the ePrivacy Directive. The penalties provided for must be "effective, proportionate and dissuasive."[682]

Furthermore, Member States have to ensure that the competent national authorities have the necessary investigative powers and resources[683] as well as the power to order the cessation of the infringements. [684]

4.1.10. Comparative Assessment

Since many of the policies discussed *supra* attempt to address the threat of "identity theft," a more detailed analysis of this phenomenon is provided in the ensuing chapter.

The subsequent chapters will provide a comparative analysis of the different regulatory regimes with regard to (1) whether they implement a sector-specific or information type-specific approach (see chapter 4.1.10.2); (2) whether they protect information confidentiality,

2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, at 12, 35, COM (2007) 698 final (Nov. 13, 2007).

[680] Council Common Position (EC) No. 16/2009 of 16 Feb. 2009, art. 2(8), 2009, O.J. (C 103 E) 40, 60 (proposing that the Commission may only adopt recommendations).

[681] *Position of the European Parliament adopted at second reading on 6 May 2009*, P6_TA(2009)0360 (May 6, 2009). ePrivacy Directive art. 15a(4) as adopted only provides that if national regulatory authorities choose to adopt measures to ensure effective cross-border cooperation, they have to notify the Commission which "may […] make comments or recommendations thereupon."

[682] *Cf. Commission Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation*, at 12, COM (2007) 698 final (Nov. 13, 2007) (stating "this enhances the implementation and enforcement mechanisms currently in place, in order to enable competent authorities to take effective and efficient action against infringements").

[683] ePrivacy Directive art. 15a(3) as amended by the CRD.

[684] ePrivacy Directive art. 15a(2) as amended by the CRD.

integrity, and/or availability (see chapter 4.1.10.3); (3) whether they require "reasonable" or certain specific safeguards (see chapter 4.1.10.4); (4) the allocation of internal responsibility (see chapter 4.1.10.5); and (5) the available enforcement mechanisms (see chapter 4.1.10.6).

4.1.10.1. Excursion: "Identity Theft"—A Misconceived Threat

"Identity theft" is commonly defined as "a fraud committed or attempted using the identifying information of another person without authority."[685] The first stage of "identity theft" involves the acquisition of identifying information such as the name, date of birth, or Social Security number of an individual.

In the second stage, the identifying information is used by criminals to commit a fraud by claiming to be the person the identifying information relates to. The two most common types of fraud are existing account fraud and new account fraud. The former occurs when the identifying information is misused to gain access to an existing credit, brokerage, banking, or utility account. The latter consists of a misuse of the identifying information to open new accounts in the name of the individual the information relates to. Existing account fraud occurs more often but causes less damage,[686] in particular to consumers, because (1) it is usually noticed and reported quickly by account holders and (2) consumers generally do not face liability for fraudulent charges.[687] New account fraud, on the other hand, can go unnoticed for months, leading to a third stage of "identity theft."

[685] 16 C.F.R. § 603.2(a) (2010). *Cf.* THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT—A STRATEGIC PLAN 10 (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf (defining "identity theft" as "the misuse of another individual's personal information to commit fraud").

[686] *See* THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT—A STRATEGIC PLAN 3 (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

[687] *See infra* chapter 5.4 (discussing the limitations on the liability of payment service users under the Truth in Lending Act, the Electronic Fund Transfer Act, and the EU's Payment Services Directive).

In the third stage, the businesses that unknowingly fall victim to the new account fraud report to credit reporting agencies that their "customer"—the individual who was impersonated by the fraudster—defaulted. The credit reporting agencies then assign a bad credit score to the consumer which may lead to less favorable credit terms or might even make it impossible for the consumer to obtain a loan or a particular job. As far as consumers are concerned, "identity theft" is therefore an information security-related threat because it compromises the integrity of their credit histories.

The architecture[688] that enables impersonation fraud—and subsequently the compromise of the integrity of an individual's credit history—has one fundamental vulnerability: weak customer authentication or, more precisely, a confusion between identification and authentication. Identification is the process "by which a user *provides* a claimed identity"[689] while authentication is the process "of establishing the *validity* of this claim."[690] Identification usually requires an individual to provide his name and date of birth, a username, an account number or some other kind of information that uniquely identifies the individual. To verify this claim of identity, three forms of authentication can be used: authentication by knowledge (something the individual *knows* such as a password), authentication by ownership

[688] *Cf.* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1251 (2003) (emphasizing the importance of an architectural perspective).

[689] *See* NIST, AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK, SPECIAL PUBLICATION 800-12, at 181 (1995), *available at* http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (defining "identification" as "the means by which a user *provides* a claimed identity to the system"). *Cf.* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 160 (4th ed. 2008) (stating that "[o]nce a person has been identified, through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is."). *Cf.* James S. Tiller, *Access Control*, *in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 93, 147 (Harold F. Tipton ed., 2007) (stating that identification "is the assertion of a unique user identity").

[690] *See* NIST, AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK, SPECIAL PUBLICATION 800-12 181 (1995), *available at* http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (defining "authentication" as "the means of establishing the *validity* of this claim [of identity]"). *Cf.* James S. Tiller, *Access Control*, *in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 93, 148 (Harold F. Tipton ed., 2007) (stating that authentication "is verifying the identity of the user").

(something the individual *has* such as a smart card), or authentication by characteristic (something the individual *is or does* such as a fingerprint or voice patterns).[691] Whatever is used for authentication (hereinafter referred to as an authenticator), for it to establish any meaningful level of trust that the individual is who she claims to be, it has to be something only the individual she claims to be knows, has, is, or does. This is why using an identifier (such as a username) for authentication purposes results in a very low level of trust: identifiers necessarily have to be shared with all entities to which an individual wishes to identify (and authenticate) herself to.[692] The more an identifier is used for authentication, the more parties will share it and the weaker the authentication will become. This is, however, exactly how "authentication" using SSNs works.[693] SSNs were introduced in 1936 and continue to be used as identifiers.[694] However, the federal government, state governments, and businesses use SSNs not only to identify but also to authenticate individuals.[695] Pursuant to USA PATRIOT

[691] *Cf.* James S. Tiller, *Access Control*, *in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 93, 149 (Harold F. Tipton ed., 2007); SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 160 (4th ed. 2008).

[692] *Cf.* BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 188 (2006) (noting that a Social Security number is a unique identifier but hardly a secret and therefore "a good number to identify me by, but a terrible one to authenticate me by").

[693] *Cf.* Cem Paya, *Quasi-Secrets: The Nature of Financial Information and Its Implications for Data Security, in* HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 121, 130 (Andrea M. Matwyshyn ed., 2009) (stating that credit card numbers and SSNs are, at best, "quasi-secrets" since they are considered highly confidential but are also associated with patterns of use that work to undermine their status as secrets). *Cf. also* Adam Shostack & Paul Syverson, *What Price Privacy (and why identity theft is about neither identity nor theft), in* ECONOMICS OF INFORMATION SECURITY 129, 138 (L. Jean Camp & Stephen Lewis eds., 2004) (noting that one cannot have meaningful trust with millions of entities that all have access to one's SSN or other identifying information).

[694] *See* http://www.socialsecurity.gov/history/ssn/ssnchron.html (last accessed Feb. 10, 2011).

[695] *See* SIMSON GARFINKEL, DATABASE NATION—THE DEATH OF PRIVACY IN THE 21ST CENTURY 18 et seq. (2000) (providing a history of the SSN). *Cf.* Cem Paya, *Quasi-Secrets: The Nature of Financial Information and Its Implications for Data Security, in* HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 121, 124 (Andrea M. Matwyshyn ed., 2009) (stating that "[t]oday the SSN is widely used as an *authenticator*: many processes assume that if you know the SSN for a particular person, then you *are that person or authorized to act on behalf of that person*"). *Cf. also* Simson L. Garfinkel, *Risks of Social Security Numbers*, COMMUNICATIONS OF THE ACM, Oct. 1995, at 146, 146 (stating that an SSN "isn't secret—and there is no way to make it that way in today's increasingly cross-indexed society"). Prohibiting the use of SSNs as the *sole*

Act[696] § 326(a)[697] and the implementing regulations,[698] it is generally still possible to open an account in another person's name by using his or her SSN, name, and date of birth.

The term "identity theft" is misleading in the sense that it implies that the problem is that an identity (or, more accurately, identifying information) is "stolen"—while the real problem is weak authentication that relies on identifiers for authentication. Furthermore, "identity theft" is also a misnomer because one's identifying information cannot be "stolen"—it may only be copied.[699] Thus, this thesis uses the term "impersonation fraud" instead of "identity theft."

Rather than understanding this type of crime as impersonation fraud and therefore focusing on how to make it more difficult to commit a fraud by using another person's identifying information (i.e. strengthening authentication), policy makers in the U.S. and the EU have adopted the "identity theft" conception and have, accordingly, focused on how to deter, prevent, and detect the "theft" of identifying information. The problem with this approach is

means of authenticating to a website does little to change this situation. *Cf.* chapter 4.1.7.1 (discussing California's and New York's SSN protection laws).

[696] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001).

[697] 31 U.S.C. § 5318(l) (2010).

[698] Customer Identification Programs for Broker-Dealers; Joint final rule, 68 Fed. Reg. 25,113 (May 9, 2003); Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks; Joint final rule, 68 Fed. Reg. 25,090 (May 9, 2003); Customer Identification Programs For Futures Commission Merchants and Introducing Brokers, 68 Fed. Reg. 25,149 (May 9, 2003); Customer Identification Programs for Mutual Funds, 68 Fed. Reg. 25,131 (May 9, 2003); *See* 31 C.F.R. § 103.121 (banks, savings associations, credit unions, and certain non-federally regulated banks); 31 C.F.R. § 103.122 (broker-dealers); 17 C.F.R. § 270.0-11, 31 C.F.R. § 103.131 (mutual funds); and 31 C.F.R. § 103.123 (futures commission merchants and introducing brokers).

[699] *See* Bruce Schneier, *Mitigating Identity Theft*, CNET.COM, Apr. 14, 2005, http://news.cnet.com/Mitigating-identity-theft/2010-1071_3-5669408.html *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 205, 205 (2008) (stating with regard to "identity theft" that "[t]he real crime here is fraud; more specifically, impersonation leading to fraud"). For the same reason, a copyrighted work cannot be "stolen" or be the subject of "piracy." In economic terms, this follows directly from the non-rival nature of information goods. *See, e.g.,* NIVA ELKIN-KOREN & ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE: THE EFFECTS OF CYBERSPACE ON THE ECONOMIC ANALYSIS OF LAW 51 (2004); LAWRENCE LESSIG, CODE: VERSION 2.0, at 181 (2006).

that a consumer's identifying information is (necessarily) available to all entities that have a need to identify him. Any attempt to protect its confidentiality (i.e. to prevent its "theft") is therefore utterly ineffective.

To address the fundamental architectural weakness that enables impersonation fraud, policy makers should rather focus on how to strengthen the procedures used to authenticate consumers before extending credit to them.

One option would be to mandate the implementation of certain authentication procedures (a form of indirect risk mitigation). More specifically, USA PATRIOT Act § 326(a)[700] could be amended to require not only the identification but also the proper authentication of customers—which would consequently prohibit the use of SSNs or other identifying information (e.g. date of birth or address) for authentication purposes.[701] For example, many EU Member States have, pursuant to Parliament and Council Directive 2005/60[702] article 3(1), adopted rather strict customer authentication requirements for credit institutions and financial institutions.[703] A process that provides strong authentication would have to rely

[700] 31 U.S.C. § 5318(l)

[701] *Cf.* Bruce Schneier, *The Anti-ID-Theft Bill That Isn't*, WIRED, Apr. 20, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/04/70690 *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 37, 39 (2008) (stating that the way to mitigate the risk of impersonation fraud "is not to make personal information harder to steal, it's to make it harder to use" and specifically that "[w]hat we really need are laws prohibiting financial institutions from granting credit to someone using your name with only a minimum of authentication").

[702] Parliament and Council Directive 2005/60, 2005 O.J. (L 309) 15 (EC).

[703] Some Member States only permit face-to-face authentication using government-issued photo IDs. Others do permit non face-to-face authentication but commonly require (1) that additional documentary evidence is provided, (2) the identity is confirmed by another institution which has already performed a face-to-face verification, or (3) that the first payment is carried out through an account opened in the customer's name. *See Commission Staff Working Document—The application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation to the identification of clients in non-face to face transactions and possible implications for electronic commerce*, at 9, SEC (2006) 1792 (Dec. 19, 2006).

on two-factor authentication.[704] The most straightforward form—which is also used in most EU Member States[705]—is a government-issued photo ID: To authenticate oneself, an individual needs her photo ID (authentication by ownership) and has to look like the person depicted on the photograph (authentication by characteristic).

Security freeze laws (sometimes also referred to as credit freeze laws) are another type of indirect risk mitigation measure which attempts to make it more difficult for an imposter to obtain credit in another person's name.

First, it has to be noted that this measure is only effective to the extent that creditors actually request the credit seeker's credit report before extending credit—this is however not always the case (e.g. payday lenders are known to seldom request credit reports).[706] Second, a security freeze in combination with a temporary lift for a certain time only reduces the time frame during which new account fraud can be committed easily—it does not provide for any authentication whatsoever. A security freeze in combination with a temporary lift for a specific creditor effectively implements an authentication mechanism. However, it is the creditor not the consumer who is being authenticated in this situation. While this certainly

[704] As explained *supra*, there are three forms of authentication: authentication by knowledge (something the individual knows such as a password), authentication by ownership (something the individual has such as a smart card), and authentication by characteristic (something the individual is or does such as a fingerprint or voice patterns). If two of these three forms are combined, the resulting authentication method is referred to as "two-factor authentication." *See* INFORMATION SECURITY MANAGEMENT HANDBOOK 3143 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (defining "two-factor authentication" as "[t]he use of two independent mechanisms for authentication; for example, requiring a smart cart and a password").

[705] An overwhelming majority of Member States—with the most notable exception of the UK—make it mandatory for their citizens to own a national identity card. *See* Council of the EU, State of play concerning the electronic identity cards in the EU Member States, 9949/10 (May 31, 2010). This enables businesses to implement robust authentication procedures.

[706] *Cf.* Consumers Union, *Protect your identity*, CONSUMER REPORTS MONEY ADVISER, July 2010, *available at* http://www.consumerreports.org/cro/money/consumer-protection/protect-your-identity/overview/index.htm (quoting Rebecca Kuehn, assistant director of the FTC's division of privacy and identity protection: "Some creditors, such as payday lenders, will give credit without getting a credit report").

makes it more difficult to commit impersonation fraud, it does not truly address the fundamental architectural weakness.

Furthermore, security freeze laws put the burden on consumers to freeze their credit reports and temporarily lift that freeze (for a specific third party) whenever they want to allow a potential creditor, employer, landlord, utility company, or other business to request their credit report.[707] Since each of the three national consumer reporting agencies charge a fee of $10 in California and $5 in New York, a single "authentication" may cost a consumer up to $30 in California and $15 in New York. The burden and cost of having to request security freezes (and temporary lifts) from all three national consumer rating agencies make a wide adoption of security freezes rather unlikely.[708] In summary, security freeze laws can therefore not be considered an appropriate policy instrument to fully address the threats related to impersonation fraud.[709]

[707] Critics of security freeze laws also argue that security freezes may cause consumers unwanted delays when they must provide third party institutions access to their credit histories. *Cf.* TARA ALEXANDRA RAINSON, CONG. RESEARCH SERV., IDENTITY THEFT LAWS: STATE PENALTIES AND REMEDIES AND PENDING FEDERAL BILLS, CRS REPORT FOR CONGRESS RL34028, at 2 (2007), *available at* http://opencrs.com/document/RL34028/2007-08-06/download/1005/.

[708] *See* Nicki K. Elgie, Note, *The Identity Theft Cat-and-Mouse Game: An Examination of the State and Federal Governments' Latest Maneuvers*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 621, 642 (2008) (stating that "[a]s a result of these limitations, the security freezes may not be taken advantage of by the average consumer"); Mark Farouk, Bill Analysis of Assembly Bill 372, 2007-08 Reg. Sess. (Cal. 2008) (stating that "[t]he cost and complexity of placing and lifting freezes are seen as significant barriers to the use of this protection against identity theft"). *Cf.* JENNIFER H. SAUER & NEAL WALTERS, AM. ASS'N OF RETIRED PERSONS, SECURITY FREEZE LEGISLATION: AWARENESS AND INCIDENCE OF PLACEMENT AMONG CONSUMERS 18+ IN SEVEN STATES 8 (2007), *available at* http://assets.aarp.org/rgcenter/consume/freeze_leg.pdf (stating that less than one percent of all respondents across the seven surveyed states—including California—indicated they currently have a security freeze placed on their credit files).

[709] Note that the effects of security freeze laws on impersonation fraud are largely still unknown. In January 2008, the FTC has sought public comments on the impact and effectiveness of security freezes. However, after having received 50 comments from various stakeholders, it has not yet published its own assessment as recommended by THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT—A STRATEGIC PLAN 52 (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf. *See* http://www.ftc.gov/os/comments/creditreportfreezes/ (last accessed Feb. 10, 2011).

Alternatives to security freeze laws as well as to requiring strong consumer authentication by amending USA PATRIOT Act § 326(a) would be (1) to prohibit the furnishing of information to credit reporting agencies if the customer has not been properly authenticated or (2) lifting the immunity from tort actions for businesses that furnish information to credit reporting agencies[710] if the customer has not been successfully authenticated.[711] Both alternatives as well as the initially proposed approach of amending USA PATRIOT Act § 326(a) would effectively require strong authentication procedures if any information is to be furnished to credit reporting agencies.

4.1.10.2. Sector-Specific v. Information Type-Specific Approaches

In particular U.S. federal law traditionally implements a sector-specific approach with regard to information privacy issues. This is largely due to individual industry arguments that their needs and practices were unique and should not be uniformly regulated.[712] However, such an

[710] *See* FCRA § 610(e), 15 U.S.C. § 1681h(e) (stating that no consumer may bring any action or proceeding "in the nature of defamation, invasion of privacy, or negligence with respect to the reporting of information against any consumer reporting agency, any user of information, or any person who furnishes information to a consumer reporting agency […] except as to false information furnished with malice or willful intent to injure such consumer"). *Cf.* McAnly v. Middleton & Reutlinger, P.S.C., 77 F. Supp. 2d 810, 814 (W.D. Ky. 1999) (stating that § 1681h(e) "is a quid pro quo grant of protection for statutorily required disclosures"); Remarks of Sen. Proxmire, 115 Cong. Rec. 33411 (1969) ("That is the quit pro quo […]"). *Cf. also* CHI CHI WU & ELISABETH DE ARMOND, FAIR CREDIT REPORTING 311 et seq. (6th ed. 2006).

[711] *See infra* chapter 9.1.3 (proposing the introduction of such a liability regime). *Cf. also* Chris Jay Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J. L. TECH. 2, 36 (2009), *available at* http://lawtechjournal.com/articles/2009/02_100406_Hoofnagle.pdf (proposing a strict liability regime for credit grantors).

[712] *Cf.* U.S. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 28 (1977) (recognizing the private sector's "strong interest in keeping [its] decisions about customers, clients, applicants, or employees"—which are often based on personal information—"free of unreasonable government interference"), *available at* http://epic.org/privacy/ppsc1977report/c1.htm; OFFICE OF TECHNOLOGY ASSESSMENT, COMPUTER-BASED NATIONAL INFORMATION SYSTEMS: TECHNOLOGY AND PUBLIC POLICY ISSUES 74 (1981) (noting that an omnibus legislation has been rejected by the executive branch for the following reasons: (1) it would be difficult to draft such legislation in a way that would achieve the desired protection without seriously hampering legitimate data processing applications; (2) the variety of systems, of applications, and of environments, ranging from large banks and insurance companies to street corner drugstores and individual homes, would be hard to accommodate with any single piece of legislation; (3) omnibus legislation could lead to the creation of another Federal regulatory agency that would exercise oversight over the information industry). *Cf. also* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 91 (1995); Joel R.

approach has often been rightly criticized as inefficient because the information security risks a policy aims to mitigate typically do not only occur within a particular sector but in all sectors which store, process, or transmit the information in question.[713]

However, all U.S. federal laws discussed above are sector-specific: the Communications Act only applies to telecommunications carriers, COPPA only to entities that commercially operate a website or an online service that is directed to children or that collects personal information from children with the actual knowledge of the operator, and the GLBA only to financial institutions the FTC, SEC, the federal banking agencies, or the NCUA, respectively, have jurisdiction over. The FCRA establishes separate safeguard requirements for consumer reporting agencies, furnishers, financial institutions and creditors, as well as card issuers. Only the FCRA's disposal requirements as refined in the FTC Disposal Rule apply—irrespective of sector—to all businesses that possess consumer information. The HIPAA Security Rule, despite its broadened scope which does not only cover health plans, health care clearinghouses, and health care providers but also to their respective business associates, is still a sector-specific measure. Of the state laws discussed above, only California's and New York's security freeze laws are sector-specific as they only apply to consumer reporting agencies. As regards the EU legislation, the ePrivacy Directive also implements a sector-

Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 501-11 (1995).

[713] *Cf.* Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1107 (2009) (stating that the sector-specific approach adopted to information privacy was roundly criticized in the wake of the 2005 security breaches and quoting an executive: "A credit card number or Social Security number has the same importance, regardless of the industry handling it"). *Cf. also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 67 (2004) (criticizing the legislative approach to information privacy in general by stating that "Congress has passed a series of statutes narrowly tailored to specific privacy problems").

specific approach by only covering providers of publicly available electronic communications services.

Information security risks are determined, *inter alia*, by the information assets that are affected should the risk materialize.[714] The nature of the entity which stores, processes, or transmits the information is, however, not a significant risk component. For example, whether the entity which stores a consumer's credit report is a bank, an insurance corporation, or a merchant typically has very little effect on the value of the information asset (to the consumer), the safeguards, vulnerabilities, threats, or threat agents and therefore does not influence the risk itself.

A policy that attempts to mitigate a particular information security risk by requiring a specific sector to implement security controls will necessarily be under-inclusive as it only addresses the risk with regard to that sector but ignores the very same risk when it occurs in other sectors. If personal information can be traded freely between different corporations and across different sectors—as it is generally the case under U.S. law[715]—this problem is further intensified: the very same information asset, facing the same threats and threat agents may legally require certain safeguards when processed by one corporation but may not require any safeguards once transmitted to another corporation.

Under-inclusion could be seen as negligible if only a comparatively small number of entities which store, process, or transmit the information asset are not covered by the policy.

[714] See the discussion of information security risk components *supra* in chapter 3.1.

[715] Note, however, that the HIPAA Privacy Rule constitutes an important exception to this rule; it generally requires an individual's prior authorization. *See* 45 C.F.R. § 164.502(a)(1)(iv). GLBA § 502(b), 15 U.S.C. § 6802(b) does not require an opt-in for the sharing of nonpublic personal information with nonaffiliated third parties but deems an opt-out mechanism sufficient.

However, this intuitive assessment is essentially only correct regarding non-malicious threat agents. Malicious threat agents, on the other hand, typically exploit the "weakest link" phenomenon of information security[716]: since a malicious threat agent does not need to find all but only one vulnerability, he will focus on those areas that are least protected, revealing security to be only as strong as the weakest link. Accordingly, very high levels of security in one area may not be truly relevant if other areas are unprotected (and are recognizable as such). A policy that only focuses on one sector but ignores all other areas in which the same information assets are stored, processed, or transmitted may therefore be far less effective than the ratio of covered and non-covered entities might suggest.

The only sector-specific policy discussed above whose effectiveness is not threatened by the "weakest link" phenomenon is the ePrivacy Directive. The transmission of traffic data or other personal information held by a provider of a publicly available electronic communications service to a non-covered entity brings the transmitted information out of the ePrivacy Directive's scope but does not leave it without legally required safeguards: the EUDPD's general safeguard requirements apply, also mandating "appropriate" safeguards.

In contrast to sector-specific policies, information type-specific policies focus on a very significant risk component: the information asset. Such policies are therefore generally better suited to effectively mitigate a particular risk. However, if information types are too narrowly defined, a web of policies may be created that is not only difficult to comply with and costly to enforce but also full of loopholes.

[716] BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 103 et seq. (2006). *Cf. also* ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 229 (2d ed. 2008).

All of the California and New York state laws—except the security freeze laws—as well as the EUDPD implement information type-specific approaches. The EUDPD is characterized by a broad material scope which covers all personal data. Similarly, the disposal requirements under California law apply to all personal information exempting, however, information that is publicly available.

The other state laws only apply to rather narrowly defined types of personal information: the SSN safeguard requirements under California and New York law obviously only apply to SSNs while the disposal requirement under New York law only applies to personal information in combination with (i) a Social Security number, (ii) a driver's license number or non-driver identification card number, or (iii) mother's maiden name, a number or code for a financial service, savings account, checking account, debit card, ATM, or an electronic serial number or personal identification number. Similarly, California Assembly Bill 1950 only requires safeguards for an individual's name in combination with: (a) her Social Security number; (b) her driver's license number or California identification card number; (c) her account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (d) medical information.

One of the objectives of these laws is the mitigation of risks to the confidentiality of identifying information that could be used to commit impersonation fraud. However, as discussed above, attempting to ensure the confidentiality of indentifying information is not a promising strategy for mitigating the risk of impersonation fraud. These narrowly defined state laws therefore create a patch-work of safeguard requirements that is neither well suited to fulfill its original purpose nor to significantly mitigate the security risks to personal information in general.

4.1.10.3. What to Protect: Confidentiality, Integrity, and/or Availability

As stated previously, information security is defined as the preservation of confidentiality, integrity, and availability of information.[717] However, depending on the nature of the information, these three objectives might not always be considered equally important. Accordingly, some of the policies discussed above only protect confidentiality, while others also cover integrity and availability.

All of the policies—except state security freeze laws—cover information confidentiality. Indeed, § 222 of the Communications Act, the state law safeguard requirements for SSNs, and the state law disposal requirements exclusively focus on this security property. GLBA, FCRA, COPPA protect not only the confidentiality but also the integrity of information. Since the state security freeze laws attempt to provide a type of authentication mechanism to prevent unauthorized additions to a consumer's credit history, they are the only policy measures to only protect the integrity but not the confidentiality of information.[718]

The general safeguard requirements under California Assembly Bill 1950, the EUDPD, and the ePrivacy Directive aim to protect the confidentiality, integrity, and availability of information. However, in accordance with the general scope of information privacy policies,[719] they only partly address the issue of availability by solely aiming to protect from permanent losses of availability.

[717] *See supra* chapter 2.1 (defining the term "information security" as used in this thesis).

[718] By itself, the prohibition on furnishing consumer reports when a security freeze is in place is an information privacy but not an information security measure; see *supra* chapter 2.2.1 for a discussion of how data protection and information privacy relate to information security.

[719] *See supra* chapter 2.2.1 (discussing the policy area of information privacy).

In contrast to most other types of personal information, personal health information has high availability requirements. Even brief temporary unavailability may lead to very severe consequences including a patient's death. Accordingly, the HIPAA Security Rule is the only measure that not only covers information confidentiality and integrity but also aims to fully protect information availability.

4.1.10.4. Requiring "Reasonable" v. Requiring Specific Safeguards

The most significant question with regard to a policy's effectiveness to actually mitigate information security risks is whether the policy requires the implementation of certain specific safeguards or the implementation of "reasonable" (or "appropriate") safeguards.

The difference between these approaches is rooted in the following fundamental question: Who should perform the detailed assessment of risks and the selection of safeguards—the policy makers or the regulated entities (supervised by enforcement bodies)?

Specific safeguard requirements as they result from a policy maker's detailed risk assessment have the advantage that they are relatively uncomplicated to comply with and easy to enforce. The true burden of a specific-safeguards-approach lies with the policy maker who has to perform a high-quality risk assessment in order to successfully mitigate security risks. In addition to the more general challenges of risk assessment which are discussed below in the context of regulated entities, policy makers may also face the following institutional problems: tunnel vision, random agenda selection, and inconsistency.[720]

[720] *See* STEPHEN BREYER, BREAKING THE VICIOUS CIRCLE: TOWARD EFFECTIVE RISK REGULATION 10 (1993). *Breyer's* analysis is based on federal regulation of substances that create health risks. However, the current state of information security regulation suggests that the same problems are surfacing in this regulatory field.

Stephen Breyer describes tunnel vision as a classic administrative disease that arises when an agency so subdivides its tasks that each employee's performance effectively carries the pursuit of a single goal too far.[721] Furthermore, disproportionate public attention to a particular security threat may also lead a regulator to "go the last mile." The resulting policies may lack cost-effectiveness or might even do more harm than good.[722]

The problem of random agenda selection is mostly created by public pressure to address a particular threat agent (e.g. "cyber terrorists"),[723] threat (e.g. "identity theft"),[724] or vulnerability (e.g. hard drives with unencrypted personal information being thrown into a dumpster).[725] It leads to policies that address particular risks in detail while ignoring equally significant risks entirely.[726] *Andrew Jaquith* generally describes this approach to risk management as "the hamster wheel of pain." The fundamental problem of this approach is that it addresses the easy parts of risk management—identifying and subsequently addressing *some* risks—but misses the most important part: the quantification and valuation of risks.[727] A particularly good example that demonstrates the problem of random agenda selection is the

[721] *Id.* at 11. In comparison to health risks, information security risks are only to a rather small extent subject to regulation. The problem of "tunnel vision" therefore arguably does not affect information security regulation to a very significant extent. However, as the regulation of information security risks increases, this is likely to change in the future.

[722] A policy may do more harm than good if it has unintended side-effects. For example, if a regulator, overly concerned with the risk that a compromised password might be used for months to gain undetected access to sensitive information, would mandate that passwords are changed every week, the net effect would likely be an increase and not a mitigation of risk because employees are likely to start writing passwords down (e.g. on post-its) to avoid the problem of having to remember a new password every week. *Cf.* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 607 (3d ed. 2003).

[723] *Cf. supra* chapter 2.3.7 (briefly discussing the risk of "cyber terrorism").

[724] *Cf. supra* chapter 4.1.10.1.

[725] Note that this problem seems particularly severe in the context of policies that mandate specific safeguards but may also arise if policy makers choose to perform a risk transfer instead of direct or indirect risk mitigation.

[726] *See* STEPHEN BREYER, BREAKING THE VICIOUS CIRCLE: TOWARD EFFECTIVE RISK REGULATION 19 (1993).

[727] *See* ANDREW JAQUITH, SECURITY METRICS: REPLACING FEAR, UNCERTAINTY, AND DOUBT 3 (2007).

disposal requirement under California law which applies to all personal information (excluding publicly available information). This policy therefore aims to protect personal information from the threat of "dumpster diving"[728] while ignoring the fact that California statutory law does not require the implementation of any safeguards for personal information if it does not fall within the narrow scope of California Assembly Bill 1950 or the safeguard requirements for SSNs. For example, the timely installation of security patches that close publicly known software vulnerabilities can be considered at least as significant as secure disposal processes. The heavy focus on vulnerabilities associated with the disposal of information is indeed hard to justify on the basis of any risk assessment. The particular nature of disposal-related vulnerabilities suggests why they received as much regulatory attention as they did: they are easily perceived by the general public and—in contrast to other vulnerabilities—are also occasionally noticed by laypersons.[729]

The third problem identified by *Stephen Breyer* is that of inconsistency. As regards the regulation of substances that create health risks, *Breyer* observes that agencies use different methods to estimate the effects of their regulations and measure the value of the assets they are trying to protect (in particular a human's life) very differently.[730] These problems are

[728] *Cf.* JOHNNY LONG, NO TECH HACKING: A GUIDE TO SOCIAL ENGINEERING, DUMPSTER DIVING, AND SHOULDER SURFING 1 (2008).

[729] *See, e.g.,* Der Spiegel, *IT-Firma versteigert Festplatte mit Millionen Kontodaten* [*IT Company Auctions off Hard Disc Containing Millions of Bank Account Records*], SPIEGEL ONLINE (F.R.G.), Aug. 26, 2008, *available at* http://www.spiegel.de/netzwelt/web/0,1518,574470,00.html; Maureen Culley & Vanessa Allen, *New data blunder as details of thousands of council taxpayers are found on £6.99 computer sold on eBay*, DAILY MAIL (U.K.), Aug. 27, 2008, *available at* http://www.dailymail.co.uk/news/article-1049413/New-data-blunder-details-thousands-council-taxpayers-6-99-sold-eBay.html; Stephen Mihm, *Dumpster-Diving for Your Identity*, N.Y. TIMES, Dec. 21, 2003, *available at* http://www.nytimes.com/2003/12/21/magazine/dumpster-diving-for-your-identity.html?partner=rssnyt&emc=rss&pagewanted=1; Jessica Salter, *Camera sold on eBay contained MI6 files*, DAILY TELEGRAPH (U.K.), Sept. 30, 2008, available at http://www.telegraph.co.uk/news/uknews/3107003/Camera-sold-on-eBay-contained-MI6-files.html.

[730] STEPHEN BREYER, BREAKING THE VICIOUS CIRCLE: TOWARD EFFECTIVE RISK REGULATION 21 et seq. (1993)

likely to appear also in the area of information security risk regulation. However, at the present time, most legislative and regulatory bodies in the U.S. and the EU do not even attempt to quantitatively measure the value of information or the effects their policies have on information security risk.[731] The inconsistencies in the area of information security regulation are therefore likely to be even greater than in the area of health risk regulation.

What further complicates a policy maker's task of establishing specific safeguard requirements is that risks may vary from one company to another. Accordingly, a specific safeguard may be suitable to address the risk of one company but may be insufficient or disproportionately expensive for another company. This issue can be partly addressed by implementing a sector-specific policy, assuming that the industry sector in question is sufficiently homogenous. For example, the telecommunications sector in the EU arguably fulfills these conditions, making additional sector-specific safeguard requirements as implemented in the ePrivacy Directive a reasonable policy choice. The HIPAA Security Rule implements a particularly interesting approach to the problem of varying security requirements: it provides a number of rather general "standards" and, for each standard, more detailed "implementation specifications." The implementation of the latter is, however, not always mandatory. Some only have to be implemented if they are "reasonable and appropriate." This creates a considerable amount of flexibility for HIPPA-covered entities and their business associates which may vary significantly with regard to their size and security capabilities.

[731] For a discussion of the (perceived) difficulty of measuring information security risks see *supra* chapter 2.4.3.

Another problem with regard to specific safeguard requirements is that information technology and, along with it, threats, vulnerabilities, and potential safeguards change quickly. The challenge for a policy maker is therefore on the one hand to draft a sufficiently detailed policy that can be enforced easily and, on the other hand, to avoid the prescription of too detailed technological solutions that are soon made obsolete by technological advances. For example, the FCC's CPNI Regulations promulgated pursuant to Communications Act § 222 explicitly require telecommunications carriers to authenticate customers by using a password before granting them online access to customer proprietary network information. Despite the fact that the CPNI Regulations where adopted in 2007, at a time when it was already commonly known that password-based single-factor authentication has numerous weaknesses, in particular as compared to various forms of two-factor authentication, the FCC mandated the use of passwords. Another example is the COPPA Rule promulgated to by the FTC in 1999. It declares the following technical security measures to be appropriate to protect the security of children's personal information: "secure web servers" and "firewalls." The combination of these rather vaguely defined measures may have been sufficient in 1999 but can hardly be considered as such today.[732]

The last point to be made with regard to the establishment of specific safeguard requirements is that policy makers may also fail to fundamentally understand a threat, potentially leading to

[732] For a number of years, it has been commonly accepted in the information security profession that firewalls are not the "silver bullet" to all network-based security risks. *See* STEPHEN NORTHCUTT ET AL., INSIDE NETWORK PERIMETER SECURITY 6 (2d ed. 2005) (discussing the importance of implementing additional security controls inside of the network that is protected by perimeter defenses); WILLIAM R. CHESWICK ET AL., FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER 11 (2d ed. 2003) (noting that perimeter security is problematic if the number of hosts within the perimeter is too large); NITESH DHANJANI ET AL., HACKING: THE NEXT GENERATION 25 et seq. (2009) (noting that the flaw with the perimeter-based approach to security is that all the insiders are assumed to be fully trustworthy and further discussing how malicious threat agents are able to exploit web application and browser flaws to launch "inside-out" attacks). *Cf. also infra* chapter 4.3.2 (discussing the problem of the overstated significance of perimeter security in the context of the NERC standards).

inherently ineffective security requirements. This danger exists, of course, irrespective of the risk treatment options chosen. However, it is most apparent in the area of specific safeguard requirements. The identification requirements under FCRA § 604, the disposal requirements under FACTA § 216 and California and New York state law, the safeguard requirements for SSNs under California and New York state law, and the safeguard requirements under California Assembly Bill 1950 are all based on the premise that the risk of impersonation fraud is best mitigated by making it more difficult to obtain personal identifiers. As discussed *supra* in chapter 4.1.10.1, this approach fails to appreciate the fundamental difference between identifiers and authenticators and, accordingly, misconceives "identity theft" as a problem of identifying information being stolen rather than as a problem of impersonation fraud enabled by weak authentication procedures.

Policies that require "reasonable" or "appropriate" instead of any specific safeguards put the burden of determining what is "reasonable" on the regulated entities and, subsequently, on the regulatory agencies and/or courts that have to enforce the policy. All of the following require "reasonable" or "appropriate" safeguards: the FTC Safeguards Rule, the SEC Safeguards Rule, the Interagency Safeguards Guidelines, and the NCUA Safeguards Guidelines promulgated pursuant to GLBA § 501(b), FCRA § 697(b), the Furnishers Rule promulgated pursuant to FCRA § 623(e), FTC Act § 5, California Assembly Bill 1950, the EUDPD, and the ePrivacy Directive. To determine what is reasonable, FTC Act § 5 as construed by the FTC, the EUDPD, and the ePrivacy Directive refer to risk presented and the cost of implementing the safeguard while the FTC Safeguards Rule, the Interagency Safeguards Guidelines, the NCUA Safeguards Guidelines, and the Furnishers Rule refer to the organization's size and the value of the information asset. The SEC Safeguards Rule and FCRA § 697(b), however, make no reference to any criteria for what is "reasonable."

Despite the fact that the different policies refer to different factors to describe their standard of "reasonableness," all policies refer, at least implicitly, to the magnitude of risk presented as the major factor. Accordingly, companies have to perform a risk assessment in all cases in order to determine whether they are in compliance. Since the number, type, and magnitude of risks typically change over time, companies—in order to verify continuous compliance—have to adopt a life cycle approach which consists of a repetitive process that involves the identification and assessment of risks, the implementation of appropriate safeguards, monitoring and reviewing the effectiveness of the safeguards, and updating the safeguards as needed.[733]

Smedinghoff therefore argues that any legal obligation to implement "reasonable" safeguards should be understood as an obligation to implement a life cycle approach as part of a comprehensive information security program (sometimes also referred to as an information security management system or ISMS).[734]

However, contrary to *Smedinghoff's* assertion, a risk assessment, the adoption of a life cycle approach, or the implementation of a comprehensive security program are not required generally but only under the FTC Safeguards Rule, the Interagency Safeguards Guidelines,

[733] This is often described as the "Plan-Do-Check-Act" process model. *See* ISO & IEC, INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS, ISO/IEC 27001:2005 § 0.2 (2005).

[734] THOMAS J. SMEDINGHOFF, INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE 54 (2008); Thomas J. Smedinghoff, *Defining the Legal Standard for Information Security: What Does "Reasonable" Security Really Mean?*, *in* SECURING PRIVACY IN THE INTERNET AGE 19, 23 (Anupam Chander et al. eds., 2008); Thomas J. Smedinghoff, *It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law*, 16 MICH. ST. J. INT'L L. 1, 33 (2007). A standardized approach to implementing and maintaining an ISMS is provided by ISO & IEC, INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS, ISO/IEC 27001:2005 (2005).

and the NCUA Safeguards Guidelines. The other regulatory measures analyzed above do not obligate regulated entities to perform a risk assessment.[735]

While this distinction may not be of relevance to consultants who—in an effort to sell their services—often quote *Bruce Schneier* as rightly stating that "security is process,"[736] it is of great significance to smaller companies which may not have sufficient resources to conduct periodic risk assessments and implement and document a life cycle approach and a comprehensive security program.

Irrespective of whether a policy requires the covered entities to perform a risk assessment as part of fulfilling their obligation to implement reasonable safeguards, the regulatory agency or court that is responsible for enforcing the requirement of reasonable safeguards upon a specific covered entity will have to perform a risk assessment. Such an assessment is therefore, in any case, at the heart of any reasonableness standard.

However, the policies discussed above do not mandate that any specific method be used to perform a risk assessment. There is also no method that is generally accepted as an industry standard.[737] Accordingly, consultants, managers, and standardization organizations have developed a wide array of risk assessment methods that vary greatly in their approach as well as in their usefulness to objectively assess the magnitude of risks.

[735] Such an assessment may, of course, be performed nonetheless by regulated entities if they wish to determine whether they have achieved compliance.

[736] *Cf.* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 84 (2000).

[737] *Cf., e.g.,* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY RISK MANAGEMENT, ISO/IEC 27005:2008, at vi (2008) (stating that "this International Standard does not provide any specific methodology for information security risk management" and noting further that "[i]t is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector").

The first and most fundamental problem is that many risk assessment methods do not produce verifiable results.[738] This is due to the wide-spread practice of expressing risks not quantitatively but qualitatively.

In a quantitative risk assessment, risks are typically expressed as a monetary value. In its most basic form, a risk is typically calculated as the Annualized Loss Expectancy (ALE) which is defined follows[739]:

*ALE = Annualized Rate of Occurrence (ARO) * Single Loss Expectancy (SLE)*

If an assessment expresses risks in quantitative terms, the accuracy of the assessment can be verified after a certain time. For example, if a company estimates the ARO to be no more than 0.5 and the SLE to be no more than $1,000,000 and, accordingly, the risk—expressed as the Annualized Loss Expectancy—to be $500,000, the assessment could be reasonably proven wrong if, after five years, the event occurred two times per year[740] or a single occurrence of the risk caused losses significantly above the estimated SLE.

If a risk is expressed quantitatively, the decision whether or not to implement a specific safeguard can also be reviewed rather easily. For example, for a safeguard that mitigates the

[738] *See* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 106 (2009). *Cf. also* Douglas D. Hubbard & Douglas A. Samuelson, *Modeling Without Measurements: How the decision analysis culture's lack of empiricism reduces its effectiveness*, OR/MS TODAY, Oct. 2009, at 26.

[739] *See, e.g.,* DOUGLAS J. LANDOLL, THE SECURITY RISK ASSESSMENT HANDBOOK 416 (2006); Carl F. Endorf, *Measuring ROI on Security, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 133, 135 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007).

[740] The probability of an event that has an ARO of 0.5 to occur two times a year in five consecutive years—i.e. the probability of the risk assessment being correct—is 0.5^2 (the probability of two occurrences in a given year) raised by the power of 5 (the number of years): 0.00003 or 0.003%.

above risk by reducing its ARO to 0.1, it would seam "reasonable" to spend up to $400,000 on that safeguard per year.[741]

A qualitative risk assessment typically uses ordinal instead of nominal scales to rank rather than value risks. Typical scales consist of verbal values such as "low," "medium," and "high" or use numerical values such as a rating between 1 and 5. A risk is often estimated by considering the probability of a risk's occurrence and its potential impact, both also being rated on an ordinal scale. The problem with such scoring methods is that it is impossible to objectively verify weather a risk assessment was correct. For example, was a risk correctly estimated to be "medium" if it materialized twice in the last six months, each time causing a damage of $150,000? This problem is caused by the nature of ordinal scales which only rank risks relative to other risks but do not objectively value them. Furthermore, the label "high" or the numerical value 4 on a 1 to 5 scale is typically interpreted very differently by different people.[742] Even if values on an ordinal scale are assigned ranges on a nominal scale (e.g. defining a "high" impact as above $10,000,000 or defining a "low" probability as below 20%), an ordinal scale will necessarily suffer from range compression[743]: if one risk has an SLE of $100,000,000 and an ARO of 1% and another has an SLE of $250,000,000 and an ARO of 15%, both would be ranked in the same category despite the fact the second risk is 37.5 times greater than the first.[744] Research even suggests that risk matrices, a particularly

[741] The value of a safeguard can be calculated by subtracting the annual cost of the safeguard from the difference between the new ALE ($100,000) and the old ALE ($500,000). *Cf.* LANDOLL, THE SECURITY RISK ASSESSMENT HANDBOOK 418 (2006).

[742] *Cf.* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 123 et seq. (2009).

[743] *See id.* at 130, 241 (discussing range compression as well as other phenomena that introduce errors when using ordinal scales).

[744] For a similar example calculation see *id.* at 131.

popular scoring method, can be "worse than useless," leading to worse-than-random decisions.[745]

Despite the fact that qualitative risk assessment methods do not produce objective and verifiable results, they continue to be promoted by standardization and certification organizations.[746] The reason qualitative methods are still used by many organizations is that either the probability or the impact of many risks is widely believed not to be measurable.[747] However, as *Hubbard* rightly argues, the belief that something—and in particular risk—is not measurable is based on a misconception about the concept, the object, or the methods of measurement.[748]

The concept of measurement can, at least in the context of having to make decisions under uncertainty, be understood as a *reduction* of uncertainty.[749] This means that the objection that the probability of a certain event or the value of information cannot be "known" is misplaced.

[745] *See* Louis Anthony Cox, *What's Wrong with Risk Matrices?*, 28 RISK ANALYSIS 497, 500 (2008) (stating that if probability and consequence values are negatively correlated and concentrated along the line probability = 0.75 − consequence, information provided by the risk matrix is worse than useless).

[746] *See* NIST, RISK MANAGEMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS, SPECIAL PUBLICATION 800-30, at 25 (2002), *available at* http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf; Todd Fitzgerald et al., *Information Security and Risk Management,* in OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 1, 58 (Harold F. Tipton ed., 2007) (stating that "[q]ualitative risk assessments produce valid results that are descriptive versus measurable"); IT GOVERNANCE INST., CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT) 4.1, at 64 (2007), *available at* http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf (stating that the likelihood and impact of all identified risks should be assessed "using qualitative and quantitative methods"); FED. FIN. INSTS. EXAMINATION COUNCIL [FFIEC], IT EXAMINATION HANDBOOK—INFORMATION SECURITY 14-15 (2006), *available at* http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf (advocating the usage of "risk ratings" such as "High," "Medium," or "Low")

[747] *Cf., e.g.,* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 93 (4th ed. 2008) (stating that "[p]urely quantitative risk analysis is not possible because the method attempts to quantify qualitative items, and there are always uncertainties in quantitative values").

[748] DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 21 et seq. (2d ed. 2010). *Cf. supra* chapter 2.4.3 (briefly discussing these misconceptions).

[749] *See id.* at 23.

Measurements often also seem impossible because there is no clear understanding of what is actually to be measured.[750] Once the object of measurement (e.g. the value of personal information) has been clearly defined, its measurement becomes practical. Lastly, things may seem immeasurable because basic measurement methods such as various sampling procedures or controlled experiments are not well understood.[751] It is a common myth that, in cases of great uncertainty, a lot of measurement data is needed to significantly reduce that uncertainty. However, the opposite is true.[752]

Another fundamental problem that affects most qualitative as well as most quantitative risk assessment methods is the failure to express uncertainty. Ironically, this is why many people prefer qualitative over quantitative methods: they rightly hold the opinion that a claim that a risk's ALE is exactly $145,510 (or any other specific monetary amount) sounds ludicrous given the great uncertainty attached to many risks' AROs and SLEs.[753] However, as discussed above, using qualitative methods does not reduce uncertainty; it only adds ambiguity to the risk assessment.[754]

When using the traditional ALE method, experts are usually prompted to give their "best estimate." However, a negative event that has a "best estimate" impact of $100,000 is not identical to an event that is estimated (with a certain confidence level) to have an impact of $10,000 to $1,000,000.

[750] *See id.* at 26. *Cf. also id.* at 188 (discussing the measurement of the risk of "brand damage").

[751] *See id.* at 28.

[752] *Cf. id.* at 110.

[753] For a critical perspective on ALE see, for example, ANDREW JAQUITH, SECURITY METRICS: REPLACING FEAR, UNCERTAINTY, AND DOUBT 31 (2007).

[754] *Cf.* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 123 (2009)

A common way to express uncertainty is to use confidence intervals. This requires stating a range (e.g. $50,000 and $75,000) and the level of confidence (e.g. 90%) that the actual value will be within the range.[755] Going one step further, *Savage* convincingly argues that all uncertain numbers should be expressed as distributions[756] which may or may not be bell-shaped.[757] While the introduction of such methods drastically increases the mathematical complexity of a risk assessment,[758] it enables the verification of the quality of the methods underlying a risk assessment: e.g., if 100 estimates are made with a confidence level of 90%, no more and no less than 90 estimates should be correct.

The significance of expressing uncertainty is well illustrated by the estimates published by the U.S. government after the Deepwater Horizon oil spill in the golf of Mexico: at first, the Government claimed that oil was leaking at a rate of 1,000 barrels per day.[759] This estimate was revised on April 28 to 5,000 barrels per day,[760] on May 27 to 12,000 to 19,000 barrels per day,[761] on June 10 to 25,000 to 30,000 barrels per day,[762] on June 15 to 35,000 to 60,000

[755] *Cf.* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 57 (2d ed. 2010)

[756] SAM L. SAVAGE, THE FLAW OF AVERAGES: WHY WE UNDERESTIMATE RISK IN THE FACE OF UNCERTAINTY 56 et seq. (2009).

[757] *Cf.* NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE 229 et seq. (2007) (discussing the fact that many distributions are incorrectly assumed to be normal distributions while they may indeed look radically different).

[758] *Cf.* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 81 (2d ed. 2010) (discussing the use of Monte Carlo simulations to make calculations with confidence intervals); SAM L. SAVAGE, THE FLAW OF AVERAGES: WHY WE UNDERESTIMATE RISK IN THE FACE OF UNCERTAINTY 27 (2009) (describing Monte Carlo simulations in simple terms).

[759] *See* Justin Gillis, *Size of Oil Spill Underestimated, Scientists Say,* N.Y. TIMES, May. 14, 2010, at A1, *available at* http://www.nytimes.com/2010/05/14/us/14oil.html.

[760] *See* Campbell Robertson & Leslie Kaufman, *Size of Spill in Gulf of Mexico Is Larger Than Thought,* N.Y. TIMES, Apr. 29, 2010, at A14, *available at* http://www.nytimes.com/2010/04/29/us/29spill.html.

[761] Press Release, U.S. Dep't of Interior, Flow Rate Group Provides Preliminary Best Estimate Of Oil Flowing from BP Oil Well (May 27, 2010), *available at* http://www.doi.gov/news/pressreleases/Flow-Rate-Group-Provides-Preliminary-Best-Estimate-Of-Oil-Flowing-from-BP-Oil-Well.cfm.

barrels per day,[763] and on August 2 to 62,000 barrels per day.[764] Since these were all "best estimates," it is not particularly surprising that each estimate lay outside the prior estimate. The usefulness of these estimates could have been greatly improved if they had been associated with a quantitatively expressed level of confidence. From the very beginning, this would have forced estimators to either state a very low level of confidence (e.g. 10%) or, more appropriately, to drastically increase their estimated maximum.

Most risk assessment methods—whether quantitative or qualitative—also fail to address the fact that humans are generally bad at estimating risks. As discussed in chapter 2.4.2, we tend to overestimate risks that are out of our control or that are associated with malicious threat agents. We furthermore use many heuristics that lead us to incorrectly assess probabilities. The round-trip fallacy, the availability heuristic, the anchoring effect, the incorrect belief in the "law of small numbers," and the base rate fallacy are all phenomena that fall into this category.[765]

In addition to the above challenges for any information security risk assessment, the assessment of risks to the security of personal information is faced with another difficulty: How to measure a risk's potential impact on personal information?

[762] Justin Gillis & Henry Fountain, *New Estimates Double Rate of Oil Flowing Into Gulf*, N.Y. TIMES, June 11, 2010, at A1, *available at* http://www.nytimes.com/2010/06/11/us/11spill.html.

[763] Joel Achenbach & David Fahrenthold, *Oil-spill flow rate estimate surges to 35,000 to 60,000 barrels a day*, WASH. POST, June 15, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/06/15/AR2010061504267_pf.html.

[764] Joel Achenbach & David A. Fahrenthold, *Oil spill dumped 4.9 million barrels into Gulf of Mexico, latest measure shows*, WASH. POST, Aug. 3, 2010, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080204695_pf.html.

[765] *See* chapter 2.4.2.

If the confidentiality of corporate data (e.g. information describing a manufacturing process protected by a trade secret) is compromised, the company's bottom line will be affected. While there may be some uncertainty as to the extent of the impact, it is clear that the impact will be a measure of the financial losses suffered by the company.

However, the policies that require "reasonable" or "adequate" safeguards also require taking into account the impact the risk may have on the individuals the personal information relates to. Individuals may suffer economic losses, immaterial damages, or even bodily harm.[766] Which of these damages are to be taken into account? And if immaterial damages are to be considered, what is the monetary value that should be assigned to a specific violation of the security of personal information? For example, what is the impact—expressed in monetary terms—of the information on the sexual orientation of 1,000 people being compromised?[767]

None of the policies discussed above provide guidance for answering these questions. They all leave it to the covered entities to decide how—or if at all—to measure the potential impact on personal information.

In summary, all of the policies discussed above that require "reasonable" or "adequate" safeguards are fundamentally flawed because they allow risk assessment methods to be used that (1) are qualitative in nature and therefore generally produce unverifiable (and bad)

[766] In particular the loss of availability or integrity of personal health information may lead to bodily harm. However, other scenarios are possible too. Compare, for example, the facts in Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1008 (N.H. 2003) (woman was killed by stalker who bought the victim's address and Social Security number from the plaintiff, an Internet-based investigation service).

[767] Some may have ethical objections to measuring privacy in monetary terms. However, given that a determination has to be made as to which safeguards are "reasonable," risks and, by extension, the impacts of risks have to be measured. *Cf.* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 39 (2d ed. 2010) (discussing ethical objections to measurement). *Cf.* STEPHEN BREYER, BREAKING THE VICIOUS CIRCLE: TOWARD EFFECTIVE RISK REGULATION 16 (1993) (discussing the question of how much to spend to save a statistical life).

results; (2) fail to express uncertainty; (3) do not address the psychological challenges humans face when estimating risks; and (4) do not provide any guidance for how to measure a risk's potential impact on personal information.[768]

Such risk assessment methods permit that policy makers can claim to have addressed the issue, consultants and manufacturers can continue to sell their products and services using "fear, uncertainty, and doubt,"[769] and businesses that store, process, or transmit personal information can rightly claim to have fulfilled their legal obligations. In such an environment, consultants and manufacturers will continue to promote their products and processes as "best practices," irrespective of whether they have any proven track record of actually mitigating risks.[770] Critically, this could be described as an eyewash.

However, this is not to say that policies that require "reasonable" safeguards cannot be effective. To make this possible, they would have to mandate the use of a specific risk assessment method that addresses all of the problems noted above. Since the development of such a method is very challenging, policy makers may choose to approach the problem in a three-step process: (1) funding research and standardization efforts; (2) assessing the quality

[768] *Cf.* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 255 (2009) (also making the point that many laws and regulations are too vague about what counts as proper risk analysis).

[769] *See* ANDREW JAQUITH, SECURITY METRICS: REPLACING FEAR, UNCERTAINTY, AND DOUBT 11 (2007) (arguing that without formal security measurement, many companies will be guided by fear, uncertainty, and doubt ("FUD")). *Cf.* ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 33 (2008) (noting that the people's fears and sense of being overwhelmed by security challenges are sometimes being taken advantage of to market IT security products); John R. Michener et. al., *"Snake-Oil Security Claims" The Systematic Misrepresentation of Product Security in the E-Commerce Arena*, 9 MICH. TELECOMM. & TECH. L. REV. 211, 213 (2003) (stating that "[v]endors have willfully taken approaches and used processes that do not allow assurance of appropriate security properties, while simultaneously and recklessly misrepresenting the security properties of their products to their customers").

[770] *Cf.* ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 36 et seq. (2008) (noting that "best practices" have proliferated within the security industry and stating that one has to consider where they come from: "they are dictated by consultants, vendors, and the security industry as a whole" whereas "[e]ach of these groups has a vested interested in the security decisions that are made").

of the emerging risk assessment standards; and (3) mandating the use of a specific standard deemed to be best suited to address the problems identified above.

4.1.10.5. Allocating Internal Responsibility

When a policy requires an organization to implement certain safeguards, the question arises, whether the organization is free to choose the organizational approach for fulfilling these obligations. This issue is significant because the management level at which compliance is primarily monitored will largely determine whether the necessary organizational awareness will be raised and sufficient funding will be made available for implementing the required safeguards.[771]

In this regard, the Interagency Safeguards Guidelines and the NCUA Safeguards Guidelines require that the financial institution's board of directors or an appropriate committee of the board approves the information security program and oversees its development, implementation, and maintenance.[772] Furthermore, a report that describes the overall status of the information security program as well as the institution's compliance with the Guidelines has to be submitted at least annually to the board or an appropriate committee.

[771] *Cf.* KRAG BROTBY, INFORMATION SECURITY GOVERNANCE: A PRACTICAL DEVELOPMENT AND IMPLEMENTATION APPROACH 12 (2009) (stating that aligning security functions directly with business objectives serves to provide greater support for and cooperation with security efforts by business owners and senior management which will in turn improve the "tone at the top" and the overall security culture); Todd Fitzgerald, *Information Security Governance, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 15, 33 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (emphasizing the importance of demonstrable executive management support for information security). *Cf. also* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, ISO/IEC 27002:2005 § 6.1 (2005) (stating that "[m]anagement should approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the organization").

[772] *Cf.* Interagency Guidelines Establishing Standards for Safeguarding Customer Information; Final Rule, 66 Fed. Reg. 8,616, 8,620 (Feb. 1, 2001) (noting that "[t]he Agencies believe that a financial institution's overall information security program is critical to the safety and soundness of the institution. Therefore, the final Guidelines continue to place responsibility on an institution's board to approve and exercise general oversight over the program").

Similarly, the Red Flags Rule mandates that the board of directors or an appropriate committee of the board approve the initial "Identity Theft Prevention Program" and that the board of directors, an appropriate committee thereof, or a designated senior manager is involved in the oversight, development, implementation and administration of the program.[773]

The FTC Safeguards Rule does not require the involvement of senior management but at least mandates that one or more employees be designated to coordinate the information security program.[774]

All other policies discussed above do not mandate that senior management or even one or more designated employees are involved in the compliance effort. However, the EUDPD explicitly allows—but does not require—Member States to provide incentives for data processors to appoint a Data Protection Official (DPO) who, whether or not an employee, must be in a position to exercise his functions in complete independence.[775] In cases where a data processor has appointed a DPO, Member States may adopt a simplification of, or exemption from the requirement to notify the Member State's supervisory authority[776] before carrying out any automatic processing of personal data.[777] It is then the DPO's—instead of the supervisory authority's—responsibility to ensure *ex ante* that the processing operations

[773] *Cf.* Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule, 72 Fed. Reg. 63,718, 63,731 n.34 (Nov. 9, 2007) (stating that these requirements are modeled on sections of the Interagency Safeguards Guidelines).

[774] *See* FTC Safeguards Rule, 67 Fed. Reg. 36,484, 36,489 (May 23, 2002) (noting that the designation of any employee—and not only senior managers—is sufficient because the FTC was "particularly concerned that small institutions not be burdened disproportionately by this paragraph").

[775] *See* EUDPD recital 49 (requiring a DPO's "complete independence"). *Cf. also* DAVID BAINBRIDGE, EC DATA PROTECTION DIRECTIVE 51, 95 (1996).

[776] *See* EUDPD art. 28.

[777] *See* EUDPD art. 18(2). Alternatively, the notification requirements may also be simplified for such data controllers. *See id.*

comply with the national data protection law.[778] Going beyond the requirements of the Directive, Germany was the only Member State to make the appointment of a DPO obligatory.[779]

To the extent that the policies discussed above allocate internal responsibility, there is a clear distinction between the EU and the U.S. approach: while U.S. policies generally attempt to ensure that internal responsibility is allocated to an individual with significant authority in the organization, the EUDPD focuses on independence from the organization. The reason for the differing approaches may be attributed to the fact, that the EUDPD's DPO is not only responsible for the compliance with security requirements but also with all other requirements under the applicable national data protection law which potentially leads to more significant conflicts between the data controller's and the data subjects' interests, thereby necessitating a certain amount of independence.[780] As regards the compliance with security requirements for personal information, it has to be emphasized that significant resources are needed to verify compliance, in particular due to the complexity and time-consuming nature of a proper risk assessment. This makes an independent DPO a less attractive policy choice than a senior manager—unless the law ensures that the DPO has the necessary resources and sufficient access to senior management, in particular by requiring that DPOs directly report to their

[778] *See* EUDPD art. 20(2). The DPO only has to consult the supervisory authority in cases of doubt. *See id*. *Cf. also* EUDPD recital 49.

[779] *See* Bundesdatenschutzgesetz [Federal Data Protection Act], Jan. 14, 2003, BGBl. I at 66, as amended, § 4f(1) (F.R.G.). France, the Netherlands, Belgium, Luxembourg, and Sweden made the appointment of a DPO voluntary, offering an exemption from the notification requirement as an incentive. *Cf.* DOUWE KORFF, EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE—COMPARATIVE SUMMARY OF NATIONAL LAWS 165, 168 (2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf; RAMBØLL MANAGEMENT, ECONOMIC EVALUATION OF THE DATA PROTECTION DIRECTIVE 95/46/EC 17 (2005), *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/economic_evaluation_en.pdf.

[780] Historically, the policy innovation of a (mandatory) DPO can be traced back to Bundesdatenschutzgesetz [Federal Data Protection Act], Feb. 1, 1977, BGBl. I at 201, 209, § 28 (F.R.G.).

CEOs—as is the case under German law.[781] Germany therefore allocates internal responsibility in a way that combines the EU and the U.S. approach, that is to require that the appointed individual has both, a certain amount of influence (in terms of access to the CEO) and independence.

4.1.10.6. Enforcement Mechanisms

All of the policies that require personal information controllers to implement safeguards exclusively provide for public enforcement mechanisms.

The FTC Safeguards Rule, the SEC Safeguards Rule, the Interagency Safeguards Guidelines, and the NCUA Safeguards Guidelines promulgated pursuant to GLBA § 501(b), the FCC's CPNI Regulations adopted pursuant to § 222 of the Communications Act, and FTC Act § 5 only task the respective regulatory agencies with enforcing the security requirements. Going one step further, the HIPAA Security Rule, the FCRA, and COPPA do not only grant (federal) regulatory agencies enforcement powers but also allow state attorneys general to bring enforcement actions in federal court.[782]

The relevant California and New York state laws are to be enforced by the state attorneys general. Similarly, the EUDPD's security requirements are to be enforced by national

[781] *See* Bundesdatenschutzgesetz [Federal Data Protection Act], Jan. 14, 2003, BGBl. I at 66, as amended, § 4f(3) (F.R.G.) (mandating that the DPO be directly subordinate to the head of the data controller) and *id.* § 4f(5) (requiring that a data controller support its DPO providing "assistants, premises, furnishings, equipment and other resources as needed to perform [his] duties"). Note that Germany law also requires the DPOs have "specialized knowledge and reliability necessary to carry out their duties." *Id.* § 4f(2). *Cf. also* DOUWE KORFF, EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE—COMPARATIVE SUMMARY OF NATIONAL LAWS 178 (2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf (noting that in Germany, DPOs are regarded as a major means towards effective implementation of the law).

[782] Note that, to a small extent, GLBA also allows enforcement by the states. Pursuant to 15 U.S.C. § 6805(a)(6), state insurance regulators are also charged with the enforcement of the GLBA's safeguards and privacy provisions insofar as they apply to insurance activities within the state regulators' jurisdiction.

supervisory authorities and those of the ePrivacy Directive by other national authorities established by a Member State.

Remarkably, none of the policies specifically provide private enforcement mechanisms. However, compliance with California state law can be enforced by competitors under California unfair competition law.[783] Similarly, some EU Member States allow competitors to bring enforcement actions with regard to the EUDPD and the ePrivacy Directive under national unfair competition law.[784]

4.2. Mandatory Security Controls for Publicly Traded Companies

This chapter discusses information security in the context of the relationship between a publicly traded company and its shareholders. From a (potential) shareholder's perspective, the security, and more specifically the integrity, of financial reports issued by the company are of paramount importance as they directly affect the shareholders' decision to buy or sell shares.

4.2.1. Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 (SOX)[785] was passed in reaction to a number of accounting scandals at publicly traded companies, in particular at Enron[786] and WorldCom.[787] The

[783] *See* Clayworth v. Pfizer, Inc., 233 P.3d 1066, 1088 (Cal. 2010) (holding that the right to seek injunctive relief under CAL. BUS. & PROF. CODE § 17203 is not dependent on the right to seek restitution).

[784] EU unfair competition law does not require Member States to grant businesses a legal right of action against competitors whose commercial practices are illegal unless those practices can also be considered "unfair." *See* Parliament and Council Directive 2005/29, art. 5(2)(b), 2005 O.J. (L 149) 22, 27 (EC) (prohibiting "unfair" commercial practices and stating that a practice is only unfair if "(a) it is contrary to the requirements of professional diligence, and (b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers").

[785] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified in scattered sections of 11, 15, 18, 28 and 29 U.S.C.)

purpose of SOX was to "protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws."[788]

The relevant provisions of SOX apply to publicly traded companies ("issuers").[789] With regard to the issue relevant in this chapter, the implementation and maintenance of security controls, this also includes smaller public companies.[790]

Two different provisions, SOX § 302[791] and § 404[792] address the issue of "internal controls" by (1) effectively mandating that controls be established and maintained and (2) requiring that certain disclosures be made regarding internal controls (see chapter 6.1.1).

SOX § 404(a) requires that annual reports filed pursuant to § 13(a) or § 15(d)[793] of the Securities Exchange Act of 1934,[794] *inter alia*, state the responsibility of management "for establishing and maintaining an adequate internal control structure and procedures for

[786] *Cf.* Richard A. Oppel Jr. & Andrew Ross Sorkin, *Enron Admits to Overstating Profits by About $600 Million*, N.Y. TIMES, Nov. 9, 2001, at C1, *available at* http://www.nytimes.com/2001/11/09/business/enron-admits-to-overstating-profits-by-about-600-million.html.

[787] *Cf.* Simon Romero & Alex Berenson, *WorldCom Says It Hid Expenses, Inflating Cash Flow $3.8 Billion*, N.Y. TIMES, June 26, 2002, at A1; Kurt Eichenwald & Seth Schiesel, *S.E.C. Files New Charges On WorldCom*, N.Y. TIMES, Nov. 6, 2002, at C1. For a general discussion of the history of SOX see JOHN T. BOSTELMAN, 1 THE SARBANES-OXLEY DESKBOOK § 2:1 et seq. (2009).

[788] 116 Stat. 745 (2002).

[789] SOX § 2(7), 15 U.S.C. § 7201(7) (2010) defines "issuer" as an issuer (as defined in Securities Exchange Act of 1934 § 3, 15 U.S.C. 78c), the securities of which are registered under § 12 of that Act (15 U.S.C. § 78l), or that is required to file reports under § 15(d) (15 U.S.C. § 78o(d)) or that files or has filed a registration statement that has not yet become effective under the Securities Act of 1933 (15 U.S.C. 77a et seq.), and that it has not withdrawn. *Cf.* JOHN T. BOSTELMAN, 1 THE SARBANES-OXLEY DESKBOOK §§ 3:2.1 (2009).

[790] The Dodd-Frank Wall Street Reform and Consumer Protection Act only narrowed § 404(b)'s personal scope of application. *See infra* chapter 6.1.1.

[791] 15 U.S.C. § 7241 (2010).

[792] 15 U.S.C. § 7262 (2010).

[793] 15 U.S.C. §§ 78m or 78o(d).

[794] Securities Exchange Act of 1934, Pub. L. No. 73-291, 48 Stat. 881 (1934) (codified at 15 U.S.C. § 78a et seq.).

financial reporting." Under the SEC's rules, these controls and procedures are referred to as "internal control over financial reporting."[795]

SOX § 302(a)(4) requires that the CFO and CEO certify in each annual or quarterly report, *inter alia*, that they are "responsible for establishing and maintaining internal controls"[796] and "have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared."[797] As "material information" may also be of a non-financial nature—and therefore not covered by "internal controls over financial reporting"—the SEC's rules introduced the term "disclosure controls and procedures"[798] to refer to the controls under § 302(a)(4).[799]

[795] *See* 17 C.F.R. §§ 240.13a-15(f) and § 240.15d-15(f) (defining "internal control over financial reporting" as "a process […] to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that: (1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer; (2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements […] and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and (3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements.").

[796] SOX § 404(a)(4)(A), 15 U.S.C. § 7241(a)(4)(A).

[797] SOX § 404(a)(4)(B), 15 U.S.C. § 7241(a)(4)(B).

[798] 17 C.F.R. §§ 240.13a-15(e) and 240.15d-15(e) (defining "disclosure controls and procedures" as "controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the [Securities Exchange Act of 1934] is recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms").

[799] *Cf.* 67 Fed. Reg. 57,276, 57,280 (Sept. 9, 2002) (stating that two different terms are used "to differentiate [the] concept of disclosure controls and procedures [used in § 302(a)(4)] from the pre-existing concept of 'internal controls' that pertains to an issuer's financial reporting and control of its assets, […] as addressed in Sections 302(a)(5) and (a)(6) and Section 404 of the Act. We make this distinction based on our review of Section 302 of the Act as well as to effectuate what we believe to be Congress' intent—to have senior officers certify that required material non-financial information, as well as financial information, is included in an issuer's quarterly and annual reports"). *Cf.* JOHN T. BOSTELMAN, 1 THE SARBANES-OXLEY DESKBOOK §§ 5:1.4, 5:6 (2009); HAROLD S. BLOOMENTHAL, SARBANES-OXLEY ACT IN PERSPECTIVE § 3:4 (2009); David S. Ruder et al., *The SEC at 70: The Securities and Exchange Commission's Pre-and Post-Enron Responses to Corporate Financial Fraud: An Analysis and Evaluation*, 80 NOTRE DAME L. REV. 1103, 1152 (2005).

From the certifications that have to be made by an issuer's CEO or CFO, an obligation for the issuer can be inferred, to implement "disclosure controls and procedures" as well as "internal control over financial reporting." This is also made explicit by the rules promulgated by the SEC.[800]

Regarding the effectiveness of the controls, the rules state that the controls have to provide "reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles ('GAAP')."[801] It has to be emphasized that, although there is a clear obligation to implement internal controls that provide "reasonable assurance," deficiencies or even material weaknesses in those controls do not necessarily constitute a violation as long as these deficiencies are disclosed to the issuer's auditors, the audit committee of the board of directors, and/or the public (see *infra* chapter 6.1.1).

While §§ 302 and 404 do not explicitly address information security, they nonetheless require security controls to assure the integrity of financial and other "material" information.[802] Specifically, the security of those IT systems that are used for storing, processing, or

[800] *See* 17 C.F.R. §§ 240.13a-15(a), 240.15d-15(a) (stating that "[e]very issuer that files reports under [Securities Exchange Act of 1934 § 15(d)] must maintain disclosure controls and procedures […] and, if the issuer either had been required to file an annual report pursuant to [Securities Exchange Act of 1934 §§ 13(a) or 15(d)] for the prior fiscal year or had filed an annual report with the [SEC] for the prior fiscal year, internal control over financial reporting").

[801] 72 Fed. Reg. 35,324, 35,326 (June 27, 2007). *See also* 17 C.F.R. §§ 240.13a-15(f) and § 240.15d-15(f) (defining "internal control over financial reporting" with reference to the "reasonable assurance" standard). *Cf.* Donald C. Langevoort, *Resetting the Corporate Thermostat: Lessons from the Recent Financial Scandals About Self-Deception, Deceiving Others and the Design of Internal Controls,* 93 GEO. L.J. 285, 315 (2004) (criticizing that "the SEC was deliberately vague about what a reasonable system of disclosure controls looks like").

[802] *Cf.* AM. BAR ASS'N, DATA SECURITY HANDBOOK 42 (2008); *Cf.* KIMBERLY KIEFER ET AL., INFORMATION SECURITY: A LEGAL, BUSINESS, AND TECHNICAL HANDBOOK 21 (2004).

transmitting relevant information is of great importance.[803] These can include servers, databases, network infrastructure, and financial applications.[804]

SOX provides very strong enforcement mechanisms as it holds senior managers personally accountable. Under the Securities Exchange Act of 1934, CEOs and CFOs who make a false or misleading statement in an application, report, or document filed pursuant to that Act are liable to any person who, in reliance upon the statement, has purchased or sold a security at a price which was affected by the statement.[805] Furthermore the certification of a statement, knowing that the periodic report accompanying the statement does not comport with all requirements, might result in criminal penalties of up to $1,000,000 or imprisonment of up to ten years, or both.[806] SEC may also seek redress,[807] which includes the possibility of cease-and-desist proceedings to prohibit individuals from serving as directors or officers of public companies.[808]

[803] *See* Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934; Final Rule, 72 Fed. Reg. 35,324, 35,328 (June 27, 2007) (stating that "[w]hile IT general controls alone ordinarily do not adequately address financial reporting risks, the proper and consistent operation of automated controls or IT functionality often depends upon effective IT general controls"). *Cf.* PUB. CO. ACCOUNTING OVERSIGHT BD. [PCAOB], AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A, at A1-18 (2007), *available at* http://pcaobus.org/Rules/Rulemaking/Docket%20021/2007-06-12_Release_No_2007-005A.pdf (stating that "[t]he identification of risks and controls within IT is not a separate evaluation. Instead, it is an integral part of the top-down approach used to identify significant accounts and disclosures and their relevant assertions, and the controls to test, as well as to assess risk and allocate audit effort as described by this standard").

[804] *See* Bonnie A. Goins, *Sarbanes–Oxley Compliance: A Technology Practitioner's Guide, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 2693, 2695 et seq. (Harold F. Tipton & Micki Krause eds., 6th ed. 2007); SANJAY ANAND, SARBANES-OXLEY GUIDE FOR FINANCE AND INFORMATION TECHNOLOGY PROFESSIONALS 28 (2006).

[805] Securities Exchange Act of 1934 §§ 13(a) and 18, 15 U.S.C. § 78m(a) and 78r.

[806] SOX § 906, 18 U.S.C. § 1350. For willful violations, the penalty is increased to up to $5,000,000, or imprisonment of up to 20 years, or both. 18 U.S.C. § 1350(c)(2).

[807] *See* Securities Exchange Act of 1934 §§ 20, 21, 21C, and 21D, 15 U.S.C. §§ 78t, 78u, 78u–3, and 78u–4.

[808] *See* 15 U.S.C. § 78u-3. *Cf.* JOHN T. BOSTELMAN, 2 THE SARBANES-OXLEY DESKBOOK § 15:1 et seq. (2009).

4.2.2. Fourth EU Company Law Directive

In particular in reaction to an accounting scandal at the Italian company Parmalat,[809] Council Directive 78/660[810] (hereinafter *Fourth Company Law Directive*) was amended by Parliament and Council Directive 2006/46[811] to "further enhance confidence in the financial statements and annual reports published by European companies."[812]

Article 46a of the amended Fourth Company Law Directive requires a company whose securities are admitted to trading on a "regulated market"[813] to include a Corporate Governance Statement in its annual report. The Corporate Governance Statement has to include, *inter alia*, "a description of the main features of the company's internal control and risk management systems in relation to the financial reporting process."[814] In stark contrast to SOX §§ 302, 404,[815] no duty to actually implement an internal control system or a risk management systems can be inferred from this disclosure obligation:

[809] *Cf.* John Hooper & Mark Milner, *Parmalat debacle predicted to cost Italian economy €11bn*, THE GUARDIAN (U.K.), Jan. 15, 2004, *available at* http://www.guardian.co.uk/business/2004/jan/15/corporatefraud.italy1. *See also Commission Communication on Preventing and Combating Corporate and Financial Malpractice*, at 3, COM (2004) 611 final (Sept. 27, 2004).

[810] 1978 O.J. (L 222) 11 (EEC) as amended.

[811] 2006 O.J. (L 224) 1 (EC).

[812] *Commission Proposal for a Directive of the European Parliament and of the Council amending Council Directives 78/660/EEC and 83/349/EEC concerning the annual accounts of certain types of companies and consolidated accounts*, at 2, COM (2004) 725 final (Oct. 27, 2004).

[813] Fourth Company Law Directive art. 46a refers to art. 4(1)(14) of Parliament and Council Directive 2004/39, 2004 O.J. (L 145) 1 (EC) as amended (defining "regulated market" as "a multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments – in the system and in accordance with its non-discretionary rules – in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is authorised and functions regularly and in accordance with the provisions of Title III [of Directive 2004/39]").

[814] Fourth Company Law Directive art. 46a(1)(c).

[815] *See supra* chapter 4.2.1.

In its proposal, the Commission emphasized that the purpose of a Corporate Governance Statement was to provide more "[i]nformation about corporate governance structures in listed European companies."[816] Similarly, recital 10 of the amending Parliament and Council Directive 2006/46 provides that a Corporate Governance Statement should include "a description of the main features of *any existing* risk management systems and internal controls," thereby hinting at the possibility that no such systems are present. Some Member States have also explicitly adopted this interpretation.[817]

Unlike U.S. federal law, EU law therefore does not impose an obligation for publicly traded companies to implement any information security controls to protect the integrity of financial information subject to mandatory reporting.

4.2.3. Assessment

The security or, more specifically, the integrity of information contained in financial reports issued by publicly traded companies is highly important for (potential) shareholders because

[816] *Commission Proposal for a Directive of the European Parliament and of the Council amending Council Directives 78/660/EEC and 83/349/EEC concerning the annual accounts of certain types of companies and consolidated accounts*, at 6, COM (2004) 725 final (Oct. 27, 2004).

[817] As regards Germany see Handelsgesetzbuch [HGB] [Commercial Code] May 10, 1897, Reichsgesetzblatt [RGBl]. 219, as amended, § 289(5) and *Gesetzentwurf der Bundesregierung zum Gesetz zur Modernisierung des Bilanzrechts (BilMoG),* BTDucks 16/10067, at 76 (F.R.G.) (explicitly stating that § 289(5) would not create an obligation to implement any internal control system). *Cf.* Klaus Wolf, *Zur Anforderung eines internen Kontroll- und Risikomanagementsystems im Hinblick auf den (Konzern-) Rechnungslegungsprozess gemäß BilMoG* [*On the Requirement of an Internal Control and Risk Management System with Regard to the (Consolidated) Financial Reporting Process Pursuant to BilMoG*], 2009 DEUTSCHES STEUERRECHT 920, 921. Furthermore, Bulgaria, Ireland, The Netherlands, Poland, Romania, and The United Kingdom also do not generally require the implementation of an internal control system for all publicly traded companies. *See* LANDWELL & ASSOCIÉS, STUDY ON MONITORING AND ENFORCEMENT PRACTICES IN CORPORATE GOVERNANCE IN THE MEMBER STATES: DETAILED LEGAL ANALYSIS 32, 151, 259, 280, 316, 422 (2009), *available at* http://ec.europa.eu/internal_market/company/docs/ecgforum/studies/comply-or-explain-090923-appendix1_en.pdf. *Cf. also* RISKMETRICS GROUP ET AL., STUDY ON MONITORING AND ENFORCEMENT PRACTICES IN CORPORATE GOVERNANCE IN THE MEMBER STATES 42-43 (2009), *available at* http://ec.europa.eu/internal_market/company/docs/ecgforum/studies/comply-or-explain-090923_en.pdf (observing that "[c]ontrary to the situation in the United States, where internal control and risk management issues are heavily regulated both in law and in securities regulations, those issues have not, so far, been a central focus of European policies").

they base their decision to buy or to sell shares on that information. Accounting scandals like those at Enron and WorldCom in the U.S. and at Parmalat in the EU have clearly demonstrated the risks associated with trusting incorrect financial reports.

To (indirectly) mitigate[818] these risks, the U.S. has passed SOX § 404 which requires the implementation of "adequate" "internal control over financial reporting" and SOX § 302 which requires the implementation of "disclosure controls and procedures." These requirements are rather vague in nature and bring with it all the difficulties of determining an "adequate" level of protection discussed *supra* in chapter 4.1.10.4. However, by providing a strong enforcement mechanism in form of personal liability of the CEO and CFO, SOX §§ 302, 404 have undoubtedly made companies focus more strongly on corporate information security issues.[819]

The Fourth Company Law Directive, on the other hand, only requires a disclosure of the "main features of the company's internal control and risk management systems"[820] and does not require the implementation of any security controls. Accordingly, corporate information

[818] *Cf. supra* chapter 3.2.1.2 (describing indirect risk mitigation).

[819] *Cf.* Janine L. Spears, *How Has Sarbanes-Oxley Compliance Affected Information Security?,* 6 ISACA J. 33 (2009), *available at* http://www.isaca.org/Journal/Past-Issues/2009/Volume-6/Pages/How-Has-Sarbanes-Oxley-Compliance-Affected-Information-Security-1.aspx (noting that SOX "provided the drive that was needed to prompt business management to direct resources toward managing internal security threats and vulnerabilities"); Lawrence A. Gordon, *The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities*, 25 J. OF ACCT. AND PUB. POL'Y 503, 528 (2006) (demonstrating that SOX has a positive impact on the voluntary disclosure of information security activities and noting that this provides indirect evidence that such activities are receiving more focus since the passage of SOX). *But see* Swapna Velichety et al., *Company Perspectives on Business Value of IT Investments in Sarbanes-Oxley Compliance*, 1 ISACA J. 42 (2007), *available at* http://www.isaca.org/Journal/Past-Issues/2007/Volume-1/Pages/Company-Perspectives-on-Business-Value-of-IT-Investments-in-Sarbanes-Oxley-Compliance.aspx (finding that there are significant differences regarding how companies perceive the business value of their IT investments for SOX compliance).

[820] Fourth Company Law Directive art. 46a(1)(c).

security with regard to financial reporting is not likely to receive the same level of attention (and funding) in the EU as it does in the U.S.[821]

4.3. Mandatory Security Controls for Service Providers

This chapter analyses regulatory policies that require service providers to implement security controls. However, policies that exclusively aim to protect the security of personal information and therefore only address service providers in their capacity as personal information controllers are not discussed here but in chapter 4.1.[822]

As discussed *supra* in chapter 2.3.1, providers of communications services and related services are of particular relevance as the availability of their services is often a precondition for the availability of most electronically stored information. Policies that address this type of service providers are discussed in the following chapters 4.3.1 and 4.3.2.

Chapter 4.3.3 will then discuss mandatory security controls as they apply to a specific type of service provider heavily regulated under EU law—certification-service providers.

4.3.1. The EU Telecoms Framework Directive

As discussed in chapter 2.3.1, the availability of the communications services offered by Internet access providers and Internet backbone providers[823] has become a *conditio sine qua non* for the availability of most electronically stored information.

[821] No comparative studies exist on this point.

[822] This applies in particular with regard to the CPNI Regulations adopted pursuant to Communications Act § 222 (*see supra* chapter 4.1.5) and ePrivacy Directive art. 4 (*see supra* chapter 4.1.9).

[823] *Cf. supra* chapter 2.3.1 (discussing both Internet access providers and Internet backbone providers).

However, until 2009, EU law did not mandate any security controls for communications service providers other than for providers that operated the public switched telephone network (PSTN).[824] U.S. law, to this day, does not require communications service providers to implement any security controls to ensure the availability of their services.

In 2009, Parliament and Council Directive 2009/140[825] (hereinafter *Better Regulation Directive* or *BRD*) introduced such an obligation for certain communications service providers by amending Parliament and Council Directive 2002/21[826] (hereinafter *Telecoms Framework Directive*). The BRD was adopted as part of the "Telecoms Package"[827] and has to be transposed by Member States by May 25, 2011.[828]

Article 13a(1) of the Telecoms Framework Directive as amended by the BRD requires Member States to ensure that providers of "public communications networks"[829] as well as providers of "publicly available electronic communications services"[830] take "appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services."[831]

[824] *See* Parliament and Council Directive 2002/22, art. 23, 2002 O.J. (L 108) 51, 65 (EC) (stating that "Member States shall take all necessary steps to ensure the integrity of the public telephone network at fixed locations and, in the event of catastrophic network breakdown or in cases of force majeure, the availability of the public telephone network and publicly available telephone services at fixed locations"), *repealed by* Parliament and Council Directive 2009/136, art. 1(14), 2009 O.J. (L 337) 11, 25.

[825] 2009 O.J. (L 337) 37 (EC).

[826] 2002 O.J. (L 108) 33 (EC).

[827] This legislative package consists of three legal acts: the Better Regulation Directive, Parliament and Council Directive 2009/136, 2009 O.J. (L 337) 11 (EC) (discussed partly *supra* in chapter 4.1.9 and *infra* in chapter 6.2.9), and Parliament and Council Regulation 1211/2009, 2009 O.J. (L 337) 1 (EC).

[828] *See* BRD art. 5.

[829] *See supra* chapter 4.1.9 (discussing the term "provider of public communications networks").

[830] *See id.* (discussing the term "provider of publicly available electronic communications services").

[831] Telecoms Framework Directive art. 13a(1).

Since the BRD notes the importance of the "functioning and availability of the physical infrastructures that deliver important services to EU citizens"[832] and the legislative history emphasizes the reliability[833] and resilience[834] of electronic communications networks and services, but does not mention the confidentiality or integrity of communications traffic in the context of article 13a, the term "security," as it is used here, has to be construed as only establishing requirements regarding the availability of communications networks and services but not regarding the confidentiality or integrity of communications traffic—which is addressed by article 4 of the ePrivacy Directive.[835]

Furthermore, article 13a(2) requires that providers of public communications networks take "all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks."[836] This integrity requirement that only applies to network providers but not to service providers should be construed as merely clarifying that the BRD did not intend to loosen the preexisting security requirements that were based on the concept of network integrity.[837] However, "network integrity" is only a

[832] BRD recital 44.

[833] *Commission Proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services*, at 9, COM (2007) 697 final (Nov. 13, 2007).

[834] *See id.* at 3. *Cf. also supra* chapter 2.1 (discussing the concepts of reliability and resilience and their relation to information security and, in particular, information availability).

[835] *See supra* chapter 4.1.9.

[836] Telecoms Framework Directive art. 13a(2).

[837] *See Commission Proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services*, at 9, COM (2007) 697 final (Nov. 13, 2007) (noting that the new provisions in art. 13b(2) "extend the scope of integrity requirements beyond telephone networks to cover mobile and IP networks"). *Cf.* Parliament and Council

precondition for availability of communications services.[838] Accordingly, both of the first two subsections of article 13a must be construed as establishing a coherent obligation to take "appropriate" measures to ensure the availability of communications networks and services. To determine what is "appropriate," the state of the art and the existing risks have to be considered.[839] To provide more guidance by setting an EU-wide minimum standard, the Commission may adopt[840] appropriate technical implementing measures.[841] However, as of this writing, no such measures have been adopted.

To enforce the regulatory requirements under article 13a, Telecoms Framework Directive article 13b mandates that the competent national regulatory authorities be given the power to (1) issue binding instructions to providers,[842] (2) require providers to disclose the information that is needed to assess the security and/or integrity of their services and networks,[843] and (3) require providers to submit, at their own expense, to a security audit carried out by a qualified independent body or a competent national authority and make the results thereof available to the national regulatory authority.[844] More generally, national regulatory authorities also have

Directive 2002/22, art. 23, 2002 O.J. (L 108) 51, 65 (EC) (addressing the "integrity of the public telephone network at fixed locations"), *repealed by* Parliament and Council Directive 2009/136, art. 1(14), 2009 O.J. (L 337) 11, 25.

[838] *Cf.* Parliament and Council Directive 2002/22, art. 23, 2002 O.J. (L 108) 51, 65 (EC) (entitled "Integrity of the network"), *repealed by* Parliament and Council Directive 2009/136, art. 1(14), 2009 O.J. (L 337) 11, 25 (EC) (*inter alia* changing the title of art. 23 to "Availability of services").

[839] *See* Telecoms Framework Directive art. 13a(1).

[840] Telecoms Framework Directive art. 13a(4) stipulates that the implementing measures must be adopted in accordance with the "regulatory procedure with scrutiny" provided for in art. 5a Council Decision 1999/468, 1999 O.J. (L 184) 23 (EC), as amended. *Cf. also* BRD recitals 75 and 76.

[841] *See* Telecoms Framework Directive art. 13a(4).

[842] *See* Telecoms Framework Directive art. 13b(1).

[843] *See* Telecoms Framework Directive art. 13b(2)(a).

[844] *See* Telecoms Framework Directive art. 13b(2)(b).

to be given "all the powers necessary to investigate cases of non-compliance and the effects thereof on the security and integrity of the networks."[845]

Furthermore, Telecoms Framework Directive article 21a requires Member States to provide penalties applicable to infringements of national provisions adopted pursuant to the Directive. These penalties must be "appropriate, effective, proportionate and dissuasive."[846]

4.3.2. NERC Standards

The U.S. Energy Policy Act of 2005[847] added § 215[848] to the Federal Power Act[849] which grants the Federal Energy Regulatory Commission (FERC) the authority to impose mandatory reliability standards on users, owners and operators of the bulk-power system.[850] These standards fall within the area of information security regulation to the extent that they address the security of information, in particular by establishing security requirements for computer systems that are used to monitor and control the bulk-power system (referred to as *Supervisory Control and Data Acquisition*, or *SCADA* systems). Recent attacks on SCADA

[845] *See* Telecoms Framework Directive art. 13b(3).

[846] Telecoms Framework Directive art. 21a.

[847] Pub. L. No. 109-58, 119 Stat. 594 (2005).

[848] Federal Power Act § 215, 16 U.S.C. § 824o (2010).

[849] Pub. L. No. 66-280, 41 Stat. 1063 (1920) (codified at 16 U.S.C. § 791 et seq., as amended).

[850] Federal Power Act § 215(b), 16 U.S.C. § 824o(b) (stating that "[a]ll users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section"). *See* Federal Power Act § 215(a)(1), 16 U.S.C. § 824o(a)(1) (defining "bulk-power system" as: "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy.").

systems by a malware known as "Stuxnet" have highlighted the importance of information security as regards utility companies.[851]

However, FERC may not exercise the authority to issue mandatory reliability standards directly but has to appoint an Electric Reliability Organization (ERO)[852] the purpose of which is to establish and enforce reliability standards for the bulk-power system, subject to FERC review: The ERO has to file proposed reliability standards with FERC[853] which may approve the standards if it determines that they are "just, reasonable, not unduly discriminatory or preferential, and in the public interest."[854] Furthermore, FERC, upon its own motion or upon complaint, may order the ERO to submit for approval a proposed reliability standard or a modification to a reliability standard.[855] If the ERO does not comply with an order, FERC may assess penalties or suspend or rescind the ERO's authority.[856]

[851] Stuxnet is a specialized malware targeting SCADA systems running Siemens SIMATIC WinCC or SIMATIC Siemens STEP 7 software. It propagates via USB-drives or open network shares by exploiting the vulnerabilities CVE-2010-2568, CVE-2010-2729, and CVE-2008-4250 in the Windows operating system. *See* NICOLAS FALLIERE ET AL., SYMANTEC CORP., W32.STUXNET DOSSIER (2010), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[852] *Cf.* Federal Power Act § 215(a)(2), 16 U.S.C. § 824o(a)(2) (defining the term "Electric Reliability Organization").

[853] *See* Federal Power Act § 215(d)(1), 16 U.S.C. § 824o(d)(1).

[854] Federal Power Act § 215(d)(2), 16 U.S.C. § 824o(d)(2).

[855] Federal Power Act § 215(d)(5), 16 U.S.C. § 824o(d)(5). *Cf.* FERC, Order Denying Rehearing, Denying Clarification, Denying Reconsideration, and Denying Request for a Stay, 132 FERC ¶ 61,218 (Sept. 16, 2010) (directing NERC to revise its rules of procedure that pertain to the development of reliability standards in order to ensure that the process cannot be used to negate a FERC directive).

[856] *See* Federal Power Act § 215(e)(5), 16 U.S.C. § 824o(e)(5) (stating that FERC "may take such action as is necessary or appropriate against the ERO or a regional entity to ensure compliance with a reliability standard or any Commission order affecting the ERO or a regional entity"). *See also* Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards, 71 Fed. Reg. 8,662, 8,726 (Feb. 17, 2006) (stating that "possible actions include the suspension or rescission of authority or the imposition of civil penalties under the [Federal Power Act]").

The North American Electric Reliability Corporation (NERC) which is a non-governmental organization that has been formed by the electric utility industry[857] applied for and was granted the role of ERO by FERC in July 2006.[858] In March 2007, FERC issued Order No. 693, approving the first 83 reliability standards.[859] NERC had filed 107 standards but FERC declined to approve 24 of those standards and further noted that 56 of the 83 standards that were being approved would need significant improvement.[860] As of February 2011, 105 reliability standards have been approved.[861] They are grouped into 14 categories, including "Critical Infrastructure Protection" (CIP).[862]

Eight CIP standards, the first version of which were adopted by FERC in Order No. 706 in February 2008,[863] specifically address information security issues and are therefore relevant here: CIP-002 (Critical Cyber Asset Identification), CIP-003 (Security Management

[857] In the wake of the Northeast U.S. blackout in 1965, NERC was founded in 1968 as the National Electric Reliability Council. Its name was later changed to North American Electric Reliability Council to reflect its broader membership across all of North America. After becoming the ERO, NERC was renamed North American Electric Reliability Corporation (NERC). *See* JACK CASAZZA & FRANK DELEA, UNDERSTANDING ELECTRIC POWER SYSTEMS: AN OVERVIEW OF TECHNOLOGY, THE MARKETPLACE, AND GOVERNMENT REGULATION 167 (2d ed. 2010).

[858] FERC, Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing, 116 FERC ¶ 61,062 (July 20, 2006).

[859] *See* FERC Mandatory Reliability Standards for the Bulk-Power System; Final Rule, 72 Fed. Reg. 16,416, 16,598 (Apr. 4, 2007).

[860] *See id.* at 16,416.

[861] *See* http://www.nerc.com/filez/standards/Mandatory_Effective_Dates_United_States.html (last accessed Feb. 10, 2011). *Cf.* 18 C.F.R. § 40.3 (stating that the ERO must post on its website the currently effective reliability standards as approved and enforceable by FERC).

[862] The other 13 categories are: Resource and Demand Balancing (BAL), Communications (COM), Emergency Preparedness and Operations (EOP), Facilities Design, Connections, and Maintenance (FAC), Interchange Scheduling and Coordination (INT), Interconnection Reliability Operations and Coordination (IRO), Modeling, Data, and Analysis (MOD), Nuclear (NUC), Personnel Performance, Training, and Qualifications (PER), Protection and Control (PRC), Transmission Operations (TOP), Transmission Planning (TPL), and Voltage and Reactive (VAR). *Cf.* JACK CASAZZA & FRANK DELEA, UNDERSTANDING ELECTRIC POWER SYSTEMS: AN OVERVIEW OF TECHNOLOGY, THE MARKETPLACE, AND GOVERNMENT REGULATION 178 (2d ed. 2010).

[863] *See* Mandatory Reliability Standards for Critical Infrastructure Protection; Final Rule, 73 Fed. Reg. 7,368 (Feb. 7, 2008).

Controls), CIP-004 (Personnel & Training), CIP-005 (Electronic Security Perimeter(s)), CIP-006 (Physical Security of Critical Cyber Assets), CIP-007 (Systems Security Management), CIP-008 (Incident Reporting and Response Planning), and CIP-009 (Recovery Plans for Critical Cyber Assets).[864] As of this writing, the most recent version of these standards adopted by FERC is version 3 (3c in the case of CIP-006).[865]

The standards primarily establish regulatory requirements for the protection of "Critical Cyber Assets." The meaning of the term "Critical Cyber Asset" is therefore of central importance for the material scope of application of all CIP standards.[866] CIP-002 describes how "Critical Cyber Assets" are to be identified.

The term "Cyber Assets" is defined by the FERC-approved Glossary of Terms[867] as "[p]rogrammable electronic devices and communication networks including hardware,

[864] For a general discussion of these standards see DEBRA S. HERRMANN, COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS: MEASURING REGULATORY COMPLIANCE, OPERATIONAL RESILIENCE, AND ROI 307 et seq. (2007); Bonnie G. Pilewski & Christopher A. Pilewski, *NERC Compliance: A Compliance Review, in* 3 INFORMATION SECURITY MANAGEMENT HANDBOOK 163 (Harold F. Tipton & Micki Krause eds., 6th ed. 2009).

[865] Version 4 of these standards has been adopted by NERC in January 2011 and is currently awaiting approval by FERC. CIP-002-4 would define specific Critical Asset identification criteria but the wording of the substantive requirements of CIP-003 through CIP-009 would remain unchanged. Version 4 of the standards is available at http://www.nerc.com/page.php?cid=2|20 (last accessed Feb. 10, 2011).

[866] *See* Mandatory Reliability Standards for Critical Infrastructure Protection; Final Rule, 73 Fed. Reg. 7,368, 7,392 (Feb. 7, 2008) (emphasizing that CIP-002 acts as "a filter, determining whether a responsible entity must comply with the remaining CIP requirements").

[867] *See* FERC Mandatory Reliability Standards for the Bulk-Power System; Final Rule, 72 Fed. Reg. 16,416, 16,592 (Apr. 4, 2007) (approving the initial version of the Glossary). The current version of the Glossary of Terms, which also lists for each term, the date of FERC approval, is available at http://www.nerc.com/page.php?cid=2|20|283 (last accessed Feb. 10, 2011).

software, and data."[868] The term "Critical Cyber Assets" is defined as Cyber Assets essential to the "reliable operation"[869] of "Critical Assets."[870]

Accordingly, CIP-002 first requires the identification of Critical Assets[871] which are defined as "[f]acilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."[872] In a second step, a list of Critical Cyber Assets has to be developed.[873] However, CIP-002 further qualifies the term Critical Cyber Assets by stating that they have to have at least one of the following characteristics: (1) use a "routable protocol"[874] to communicate outside the Electronic Security Perimeter, (2) use a "routable protocol" within a control center, or (3) be

[868] NERC, GLOSSARY OF TERMS USED IN NERC RELIABILITY STANDARDS 11 (2010), *available at* http://www.nerc.com/page.php?cid=2|20|283.

[869] *See* Federal Power Act § 215(a)(4), 16 U.S.C. § 824o(a)(4) (defining "reliable operation" as "operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements").

[870] NERC, GLOSSARY OF TERMS USED IN NERC RELIABILITY STANDARDS 11 (2010), *available at* http://www.nerc.com/page.php?cid=2|20|283.

[871] *See* NERC, CYBER SECURITY — CRITICAL CYBER ASSET IDENTIFICATION, CIP-002-3, Requirement R2 (2009), *available at* http://www.nerc.com/files/CIP-002-3.pdf.

[872] *Id.* For the purpose of the identification of Critical Assets, a risk-based assessment methodology has to be identified and documented. *See* NERC, CYBER SECURITY — CRITICAL CYBER ASSET IDENTIFICATION, CIP-002-3, Requirement R1 (2009), *available at* http://www.nerc.com/files/CIP-002-3.pdf.

[873] *See id.* Requirement R3.

[874] In its FAQs for version 1 of CIP-002—which have not been updated for version 2 or 3—NERC states that "routable protocols are those that provide switching and routing as described by the Open System Interconnection (OSI) model Layer 3 or higher." NERC, FREQUENTLY ASKED QUESTIONS (FAQS) FOR CYBER SECURITY STANDARDS: CIP-002-1 — CYBER SECURITY — CRITICAL CYBER ASSET 5 (2006), *available at* http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.pdf. Note that OSI Layer 3 corresponds to the network layer in the TCP/IP networking model. *See supra* chapter 2.3.1 (discussing the TCP/IP networking model) and *supra* chapter 2.3.1 (discussing the basic concepts of Internet routing).

dial-up accessible.[875] This significantly reduces the material scope of application of all CIP standards.

The FAQs issued by NERC for CIP-002 give the following reason for this limitation of scope: "Critical Cyber Assets that use non-routable protocols have a limited attack scope; hence, they are less vulnerable than Critical Cyber Assets using routable protocols."[876] Contrary to this assertion—and as demonstrated by Stuxnet—the common use of USB sticks or other portable storage devices may make Cyber Assets that do not use routable protocols and are not dial-up accessible equally vulnerable as "Critical Cyber Assets." The blanket exclusion of such Cyber Assets is therefore contrary to a risk-based approach. This issue was also raised with FERC before it approved CIP-002 but it only stated that it did "not find sufficient justification to remove this [limitation of scope]."[877]

Furthermore, the limitation of scope to Cyber Assets that use routable protocols or are dial-up accessible effectively eliminates "data" as a potential Critical Cyber Asset.[878] In its Notice of Proposed Rulemaking, FERC did not address the implicit exclusion of "data" and stated that "data essential to the proper operation of a critical asset, and possibly the computer systems that produce or process that data, would be considered critical cyber assets subject to the CIP

[875] *See* NERC, CYBER SECURITY — CRITICAL CYBER ASSET IDENTIFICATION, CIP-002-3, Requirements R3.1, R3.2, and R3.3 (2009), *available at* http://www.nerc.com/files/CIP-002-3.pdf.

[876] NERC, FREQUENTLY ASKED QUESTIONS (FAQS) FOR CYBER SECURITY STANDARDS: CIP-002-1 — CYBER SECURITY — CRITICAL CYBER ASSET 5 (2006), *available at* http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.pdf.

[877] Mandatory Reliability Standards for Critical Infrastructure Protection; Final Rule, 73 Fed. Reg. 7,368, 7,397 (Feb. 7, 2008).

[878] This argument has been made by ISO/RTO Council, Ontario Power, ISO New England Inc. (ISO-NE), and Southwest Power Pool (SPP) in the rulemaking procedure. *See* Mandatory Reliability Standards for Critical Infrastructure Protection; Final Rule, 73 Fed. Reg. 7,368, 7,395 (Feb. 7, 2008).

Reliability Standards."[879] However FERC's Final Rule only states that the consideration and designation of "data" as a critical cyber asset "is an area that could benefit from greater clarity and guidance from the ERO."[880] FERC further directed NERC to develop such guidance and "to consider the designation of various types of data as a critical asset or critical cyber asset."[881] Until such guidance is developed by NERC, data is therefore generally outside of CIP-002's scope.

Building on CIP-002, CIP-003 requires that all affected organizations ("responsible entities")[882] implement the following minimum security management controls to protect Critical Cyber Assets: (1) documenting and implementing a cyber security policy;[883] (2) assigning a single senior manager with overall responsibility and authority for the CIP compliance effort;[884] (3) documenting and authorizing any exceptions from the cyber security policy;[885] (4) protecting information about Critical Cyber Assets (e.g. network topology or

[879] Mandatory Reliability Standards for Critical Infrastructure Protection, Notice of proposed rulemaking, 72 Fed. Reg. 43,970, 43,983 (Aug. 6, 2007).

[880] Mandatory Reliability Standards for Critical Infrastructure Protection; Final Rule, 73 Fed. Reg. 7,368, 7,396 (Feb. 7, 2008).

[881] *Id.*

[882] All CIP standards define the term "responsible entity"—and thereby their personal scope of application by referring to NERC, its regional entities, and the following functional entities: Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity. *See* FERC, RELIABILITY FUNCTIONAL MODEL: FUNCTION DEFINITIONS AND FUNCTIONAL ENTITIES, VERSION 5, at 9 et seq. (2009), *available at* http://www.nerc.com/files/Functional_Model_V5_Final_2009Dec1.pdf (defining these and other functional entities). *Cf. also* JACK CASAZZA & FRANK DELEA, UNDERSTANDING ELECTRIC POWER SYSTEMS: AN OVERVIEW OF TECHNOLOGY, THE MARKETPLACE, AND GOVERNMENT REGULATION 172 et seq. (2d ed. 2010) (discussing the functional entities as defined in Version 4 of the Functional Model).

[883] This policy has to address the requirements in CIP-002 through CIP-009, be readily available to all relevant personnel, and be annually reviewed and approved by management. NERC, CYBER SECURITY — SECURITY MANAGEMENT CONTROLS, CIP-003-3, Requirement R1 (2009), *available at* http://www.nerc.com/files/CIP-003-3.pdf.

[884] *Id.*, Requirement R2.

[885] *Id.*, Requirement R2.

security configuration information);[886] (5) documenting and implementing a program for managing access to such information;[887] and (6) establishing and documenting change control and configuration management process.[888]

CIP-004 requires the following security controls with regard to personnel that have authorized logical or unescorted physical access to Critical Cyber Assets: (1) implementing and maintaining a security awareness program that includes security awareness reinforcement on at least a quarterly basis;[889] (2) implementing and maintaining an annual cyber security training program;[890] (3) implementing a personnel risk assessment program that is conducted for all personnel before granting any access to them;[891] (4) maintaining lists of personnel with authorized physical or logical access to Critical Cyber Assets and revoking such access within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access.[892]

These security requirements exhibit two significant deficiencies. First, a prerequisite for any personnel risk assessment is the proper authentication of personnel. However, CIP-004 deems

[886] Additionally, this also includes, at a minimum and regardless of media type, operational procedures, lists as required in CIP-002, topology diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, and incident response plans. *See id.*, Requirement R4.

[887] *See id.*, Requirement R5.

[888] *See id.*, Requirement R6.

[889] *See* NERC, CYBER SECURITY — PERSONNEL & TRAINING, CIP-004-3, Requirement R1 (2009), *available at* http://www.nerc.com/files/CIP-004-3.pdf.

[890] In particular, the training program has to ensures that all personal are trained prior to their being granted any access to Critical Cyber Assets. *See id.*, Requirement R2.

[891] *See id.*, Requirement R3.

[892] *See id.*, Requirement R4.

the usage of a Social Security number (SSN) for authentication purposes sufficient.[893] As discussed in chapter 4.1.10.1, any authentication procedure based on a person's SSN is fundamentally flawed.

Second, the access rights of personnel that have been terminated for cause only have to be revoked within 24 hours of the termination. This bright-line rule is easy to enforce but may be highly inadequate in high-risk situations. In comparison, ISO 27002 provides that access rights should be revoked *before* the employment terminates, depending on the evaluation of risk factors such as (1) the reason of termination, (2) the current responsibilities of the individual, and (3) the value of the assets currently accessible.[894]

CIP-005 in general requires the identification and protection of the "Electronic Security Perimeter" (hereinafter *ESP*) which is defined as "[t]he logical border surrounding a network to which Critical Cyber Assets are connected."[895] CIP-005 is therefore only concerned with logical access control (often also referred to as technical access control) but not with physical access control, which is the subject of CIP-006 discussed *infra*.[896]

First, CIP-005 requires that every Critical Cyber Asset resides within an ESP and that all ESPs and ESP access points are identified and documented.[897] Furthermore, all Cyber Assets

[893] *See id.*, Requirement R3.1 (naming "Social Security Number verification in the U.S." as an example of a permissible identity verification procedure).

[894] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, ISO/IEC 27002:2005 § 8.3.3 (2005).

[895] *See* NERC, GLOSSARY OF TERMS USED IN NERC RELIABILITY STANDARDS 16 (2010), *available at* http://www.nerc.com/page.php?cid=2|20|283.

[896] *Cf.* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 160 (4th ed. 2008) (noting that, in the context of access control, the terms "logical" and "technical" are often used interchangeably).

[897] NERC, CYBER SECURITY — ELECTRONIC SECURITY PERIMETER(S), CIP-005-3, Requirement R1 (2009), *available at* http://www.nerc.com/files/CIP-005-3.pdf.

(whether critical or not) that are used for access control to and/or monitoring of the ESPs have to be protected in accordance to CIP-002 through CIP-009.[898] Other non-critical Cyber Assets that reside within a defined ESP but are not used for access control and/or monitoring only have to be identified.[899] The FAQs for version 1 of CIP-005—which have not been updated for version 2 or 3—rightly explain that access points for access to non-critical Cyber Assets that reside within the same ESP as Critical Cyber Assets are important because "[n]on-critical Cyber Assets provide a jumping-off point for attack to any asset within the perimeter."[900]

Second, CIP-005 requires the implementation and documentation of administrative and technical security measures that control electronic access at all electronic access points to the ESPs.[901] Specifically, access has to be denied by default (requiring that access permissions be granted explicitly)[902] and may only be enabled for ports and services[903] required for operations and for monitoring Cyber Assets within the ESP.[904] Moreover, dial-up access to

[898] *See id.*, Requirement R1.5.

[899] See *id.*, Requirement R1.4 which states that any non-critical Cyber Asset within a defined ESP shall be identified and protected pursuant to the requirements of CIP-005. However, CIP-005 only establishes protection requirements for non-critical Cyber Assets if they are used for access control and/or monitoring of ESPs.

[900] NERC, FREQUENTLY ASKED QUESTIONS (FAQS) FOR CYBER SECURITY STANDARDS: CIP-005-1 — CYBER SECURITY — ELECTRONIC SECURITY 9 (2006), *available at* http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-005-1_FAQs_20090217.pdf.

[901] *See* NERC, CYBER SECURITY — ELECTRONIC SECURITY PERIMETER(S), CIP-005-3, Requirement R2 (2009), *available at* http://www.nerc.com/files/CIP-005-3.pdf.

[902] *See id.*, Requirement R2.1. This is a very basic security design principle, the adherence to which is a prerequisite for establishing any meaningful level of security. *See* ELIZABETH D. ZWICKY ET AL., BUILDING INTERNET FIREWALLS 64 (2d ed. 2000) (discussing the importance of a default deny stance).

[903] The term "port" refers to a TCP or UDP port (e.g. port 80 for HTTP) and the term service refers to server software providing services on one of the four TCP/IP network layers. *See* chapter 2.3.2 (briefly discussing ports in the context of the TCP/IP networking model).

[904] *See* NERC, CYBER SECURITY — ELECTRONIC SECURITY PERIMETER(S), CIP-005-3, Requirement R2.2 (2009), *available at* http://www.nerc.com/files/CIP-005-3.pdf. This requirement follows directly from the very basic security design principle of least privilege, according to which users and the processes should have the least number of privileges needed to perform their tasks. *See* Jerome H. Saltzer & Michael D. Schroeder, *The Protection of Information in Computer Systems*, 63 PROCEEDINGS OF THE IEEE 1278, 1282 (1975) (introducing

the ESP has to be secured and, where external interactive access to the ESP has been enabled, strong security controls have to be implemented to authenticate any accessing parties—given that such authentication is "technically feasible."[905] Appropriate use banners for interactive access attempts are also subject to a Technical Feasibility Exception (TFE).[906] In this context, it has to be pointed out that TFEs must be approved by NERC.[907] They may be obtained if, *inter alia*, strict compliance is technically impossible, it would require "the incurrence of costs that far exceed the benefits to the reliability,"[908] or if NERC posted a Class-Type TFE[909] on its website that covers the issue in question.[910] A TFE will only be granted if the responsible entity implements compensating measures.[911]

the principle of least privilege). *Cf. also* ELIZABETH D. ZWICKY ET AL., BUILDING INTERNET FIREWALLS 59 (2d ed. 2000) (discussing the importance of a least privilege in the context of firewall design).

[905] *See* NERC, CYBER SECURITY — ELECTRONIC SECURITY PERIMETER(S), CIP-005-3, Requirements R2.3, R2.4 (2009), *available at* http://www.nerc.com/files/CIP-005-3.pdf. *See infra* (discussing this and other technical feasibility exceptions).

[906] *See* NERC, CYBER SECURITY — ELECTRONIC SECURITY PERIMETER(S), CIP-005-3, Requirement R2.6 (2009), *available at* http://www.nerc.com/files/CIP-005-3.pdf.

[907] NERC, PROCEDURE FOR REQUESTING AND RECEIVING TECHNICAL FEASIBILITY EXCEPTIONS TO NERC CRITICAL INFRASTRUCTURE PROTECTION STANDARDS, APPENDIX 4D TO THE RULES OF PROCEDURE § 1.1 (2010), *available at* http://www.nerc.com/files/Appendix4D_TFE_Procedures_01212010.pdf (approved by FERC, Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, 130 FERC ¶ 61,050 (Jan. 21, 2010)).

[908] Note that NERC's Rules of Procedure do not state how reliability benefits should be quantified as to make this determination. *Cf.* FERC, Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, 130 FERC ¶ 61,050, at 9 (Jan. 21, 2010) (noting this deficiency and directing NERC to "to specify the manner in which reliability benefits are intended to be quantified").

[909] *See* NERC, PROCEDURE FOR REQUESTING AND RECEIVING TECHNICAL FEASIBILITY EXCEPTIONS TO NERC CRITICAL INFRASTRUCTURE PROTECTION STANDARDS, APPENDIX 4D TO THE RULES OF PROCEDURE § 2.6 (2010), *available at* http://www.nerc.com/files/Appendix4D_TFE_Procedures_01212010.pdf (defining "Class-Type TFE" as "[a] type or category of equipment, device, process or procedure for which NERC has determined that a TFE from an Applicable Requirement is appropriate, as set forth on a list of such Class-Type TFEs posted on the NERC Website"). *Cf. also* FERC, Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, 130 FERC ¶ 61,050, at 7 (Jan. 21, 2010) (voicing concerns that "the formulation of Class-Type TFE categories could undermine [FERC's] determination that TFEs should be reviewed on a case-by-case basis).

[910] *See* NERC, PROCEDURE FOR REQUESTING AND RECEIVING TECHNICAL FEASIBILITY EXCEPTIONS TO NERC CRITICAL INFRASTRUCTURE PROTECTION STANDARDS, APPENDIX 4D TO THE RULES OF PROCEDURE § 3.1 (2010), *available at* http://www.nerc.com/files/Appendix4D_TFE_Procedures_01212010.pdf. Other circumstances

Third, electronic or manual processes for monitoring and logging access at access points have to be implemented and documented.[912] Where "technically feasible," this entails (1) implementing such monitoring processes at each access point to dial-up accessible Critical Cyber Assets that use non-routable protocols[913] and (2) implementing an intrusion detection system (IDS)[914] at all access points.[915] If the implementation of an IDS is not "technically feasible," the access logs have to be reviewed at least every ninety calendar days.[916]

Lastly, a cyber vulnerability assessment of the electronic access points to the ESP has to be performed at least annually[917] and all documentation to support compliance with CIP-005 has to be reviewed, updated, and maintained at least annually.[918]

under which a TFE may be granted are: (1) strict compliance is operationally infeasible or could adversely affect reliability of the Bulk Electric System to an extent that outweighs the reliability benefits of strict compliance; (2) strict compliance cannot be achieved within the required time due to "factors such as, for example, scarce technical resources, limitations on the availability of required equipment or components, or the need to construct, install or modify equipment during planned outages"; (3) strict compliance would pose safety risks or issues that outweigh the reliability benefits of strict compliance; or (4) strict compliance would conflict with, or cause non-compliance with, a separate statutory or regulatory requirement. *See id.*

[911] *See id.* at § 3.2. Note that, according to FERC, compensating measures have to protect the reliability of the Bulk-Power System to "an equal or greater degree" than strict compliance would. *See* FERC, Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, 130 FERC ¶ 61,050, at 6 (Jan. 21, 2010). However, some requirements (e.g. proper user authentication) have no equally effective alternative, making this requirement impossible to comply with in some situations.

[912] *See* NERC, CYBER SECURITY — ELECTRONIC SECURITY PERIMETER(S), CIP-005-3, Requirement R3 (2009), *available at* http://www.nerc.com/files/CIP-005-3.pdf.

[913] *See id.*, Requirement R3.1.

[914] Specifically, this refers to a network intrusion detection system (NIDS). *Cf. generally* STEPHEN NORTHCUTT ET AL., INSIDE NETWORK PERIMETER SECURITY 159 (2d ed. 2005) (discussing the benefits of implementing a NIDS); STEPHEN NORTHCUTT & JUDY NOVAK, NETWORK INTRUSION DETECTION (3d ed. 2002) (providing a great introduction to this topic).

[915] *See* NERC, CYBER SECURITY — ELECTRONIC SECURITY PERIMETER(S), CIP-005-3, Requirement R3.2 (2009), *available at* http://www.nerc.com/files/CIP-005-3.pdf.

[916] *See id.*

[917] *See id.*, Requirement R4. The assessment has to include, at a minimum: (1) a documentation of the vulnerability assessment process, (2) a review that only ports and services required for operations at these access points are enabled, (3) discovery of all ESP access points, (4) review of controls for default accounts, passwords, and network management community strings (the latter refers to a weak authentication mechanism used by the

In summary, CIP-005 addresses all major areas of logical perimeter security but nevertheless contains two significant deficiencies: The first one consists in the fact that authentication is not an absolute requirement in case interactive access to ESPs is available externally; it only has to be performed if "technically feasible." However, unauthenticated external access drastically increases the risks to Critical Cyber Assets and should therefore not be permitted in any case.[919] If authentication is indeed technically infeasible, the external connection should be disabled rather than foregoing the security benefits of authentication.

The second deficiency of CIP-005 consists in only requiring the implementation of an intrusion detection system (IDS) if "technically feasible."[920] However, an IDS, like proper authentication for external access, should be considered mandatory without exception since it is the only way to ensure, with any reasonable level of certainty, that intrusions will be detected in a timely manner.[921] The compensating security control of performing a log review every 90 days is flatly inadequate since ESPs containing Critical Cyber Assets that are

Simple Network Management Protocol, version 1 and 2c; *cf.* DOUGLAS R. MAURO & KEVIN SCHMIDT, ESSENTIAL SNMP 21 (2005)), and (5) a documentation of the assessment results, of the action plan to mitigate identified vulnerabilities, and of the execution status of that action plan. *See id.*, Requirement R4.1-5.

[918] *See id.*, Requirement R5. After a modification of the network or of access controls, the documentation has to be updated within ninety calendar days. *See id.*, Requirement R5.2. Electronic access logs have to be retained for at least ninety calendar days. *See id.*, Requirement R5.3.

[919] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, ISO/IEC 27002:2005 § 11.4.2 (2005) (discussing user authentication for external connections).

[920] NERC, CYBER SECURITY — ELECTRONIC SECURITY PERIMETER(S), CIP-005-3, Requirement R3.2 (2009), *available at* http://www.nerc.com/files/CIP-005-3.pdf.

[921] *Cf.* STEPHEN NORTHCUTT ET AL., INSIDE NETWORK PERIMETER SECURITY 159 (2d ed. 2005) (stating that "[m]ost ominously, you may never know about an attack that doesn't damage your host, but simply extracts information, such as a password file. Without intrusion detection, you will be unaware of these events until it's much too late.").

exposed even only to a moderate level of risk would necessitate at least weekly rather than quarterly log reviews.[922]

The next CIP standard to discuss is CIP-006 which generally requires the implementation of a physical security program for the protection of Critical Cyber Assets.[923] Such a physical security plan has to ensure that (1) all Cyber Assets within an ESP (as well as all Cyber Assets used for controlling and/or monitoring access to ESPs)[924] reside within an identified Physical Security Perimeter (hereinafter *PSP*);[925] (2) all physical access points to each PSP are identified and measures are taken to control entry at those access points;[926] (3) physical access to PSPs is monitored;[927] and (4) a visitor control program is implemented that entails the maintenance of a visitor log and continuous escorted access within a PSP.[928] A physical

[922] *See* ISO & IEC, Information technology – Security techniques – Code of practice for information security management, ISO/IEC 27002:2005 § 10.10.2 (2005) (stating that "[h]ow often the results of monitoring activities are reviewed should depend on the risks involved"). *See* PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, Version 2.0, at 58 (2010), *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf (stating that merchants and service providers have to "[r]eview logs for all system components at least daily"). *Cf.* Stephen Northcutt et al., Inside Network Perimeter Security 403 (2d ed. 2005) (stating that network logs should be reviewed daily); Simson Garfinkel et al., Practical Unix and Internet Security 676 (3d ed. 2003) (recommending that system logs should be reviewed at least daily).

[923] NERC, Cyber Security — Physical Security of Critical Cyber Assets, CIP-006-3c (2010), *available at* http://www.nerc.com/files/CIP-006-3c.pdf.

[924] *See id.*, Requirement R3.

[925] *See id.*, Requirement R1.1. For an introduction into physical perimeter security see R. Scott McCoy, *Perimeter Security, in* Information Security Management Handbook 1275 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007).

[926] *See* NERC, Cyber Security — Physical Security of Critical Cyber Assets, CIP-006-3c, Requirement R1.2 (2010), *available at* http://www.nerc.com/files/CIP-006-3c.pdf.

[927] *See id.*, Requirement R1.3.

[928] *See id.*, Requirement R1.6.

security plan has to be updated within thirty calendar days of any physical security system redesign or reconfiguration[929] and has to be reviewed annually.[930]

Cyber Assets that are outside of a PSP[931] but are used for controlling or monitoring access to PSPs have to be protected from unauthorized physical access as well as in accordance with CIP-002 through CIP-009.[932]

Physical access controls have to be implemented at all PSP access points by choosing one (or more) of the following access control methods: card key, special locks, security personnel, or other authentication devices such as tokens or biometrics.[933] Physical access at all PSP access points has to be monitored and unauthorized access attempts have to be reviewed immediately.[934] All physical access also has to be recorded in a log and the log has to be retained for at least 90 days.[935] Furthermore, a maintenance and testing program has to be implemented to ensure that the physical access controls as well as the monitoring and logging systems function properly.[936]

In summary, it has to be noted that CIP-006 contains a single major weakness which is, however, central to effective physical access control: even for Critical Cyber Assets exposed

[929] *See id.*, Requirement R1.7.

[930] *See id.*, Requirement R1.8.

[931] This can only apply to non-critical Cyber Assets that do not reside within an ESP.

[932] *See id.*, Requirement R2.

[933] *See id.*, Requirement R4. For a discussion of these and similar physical access control measures see Alan Brusewitz, *Computing Facility Physical Security, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1339, 1345 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007).

[934] *See* NERC, CYBER SECURITY — PHYSICAL SECURITY OF CRITICAL CYBER ASSETS, CIP-006-3C, Requirement R5 (2010), *available at* http://www.nerc.com/files/CIP-006-3c.pdf. Permissible monitoring methods are alarm systems and human observation of access points. *See id.*

[935] *See id.*, Requirement R6, R7.

[936] *See id.*, Requirement R8.

to high levels of risk, it does not require two-factor authentication.[937] Using "something that you have" (e.g. a card key) is deemed sufficient under CIP-006. One-factor authentication is, however, inadequate for high-risk assets.[938]

The standard CIP-007 ("Systems Security Management") generally requires responsible entities to define methods, processes, and procedures for securing Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an ESP.[939]

First, this entails the implementation of test procedures to ensure that changes to existing Cyber Assets (e.g. the installation of software upgrades or security patches) do not adversely affect security.[940]

Second, responsible entities have to ensure that only those ports and services required for normal and emergency operations are enabled.[941]

[937] *See id.*, Requirement R4. *Cf. supra* chapter 4.1.10.1 (briefly discussing multi-factor authentication in the context of impersonation fraud).

[938] Gerald Bowman, *Physical Security for Mission-Critical Facilities and Data Centers*, *in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1293, 1302 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (noting that "[d]ue to the ability to gain access through the unauthorized use of keys or cards, single-factor authentication is often the single point of failure in access control systems" and that "[f]or a higher level of security, one or more of the authentication factors are often combined to create two-factor or multifactor authentication").

[939] *See* NERC, CYBER SECURITY — SYSTEMS SECURITY MANAGEMENT, CIP-007-3 (2009), *available at* http://www.nerc.com/files/CIP-007-3.pdf. *Cf.* NERC, FREQUENTLY ASKED QUESTIONS (FAQS) FOR CYBER SECURITY STANDARDS: CIP-007-1 — CYBER SECURITY — SYSTEMS SECURITY MANAGEMENT 4 (2006), *available at* http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-007-1_FAQs_20090217.pdf (stating that non-critical Cyber Assets within the ESP are subject to the requirements of CIP-007 because if not protected, they can provide an open door into the network and Critical Cyber Assets). Note that the FAQs issued for version 1 of CIP-007 have not been updated for version 2 or 3.

[940] *See* NERC, CYBER SECURITY — SYSTEMS SECURITY MANAGEMENT, CIP-007-3, Requirement R1 (2009), *available at* http://www.nerc.com/files/CIP-007-3.pdf.

[941] *See id.*, Requirement R2. This requirement follows directly from the very basic security design principle of least privilege which has already been mentioned *supra* in connection with CIP-005.

Third, a security patch management program has to be implemented for tracking, evaluating, testing, and installing applicable security updates for all Cyber Assets within an ESP.[942] CIP-007 gives responsible entities 30 calendar days to assess whether a specific security update should be applied.[943] It does not, however, set a deadline for the installation of updates.

Fourth, responsible entities are required to use anti-malware software, where technically feasible, to address the risk of "introduction, exposure, and propagation of malware on all Cyber Assets within the [ESPs]."[944]

Fifth, responsible entities have to manage system accounts[945] by implementing security controls in order to authenticate all users, ensure accountability for user activity,[946] and minimize the risk of unauthorized system access.[947] *Inter alia*, a responsible entity has to manage the acceptable use of administrator, shared, and other generic account privileges.[948] As regards user authentication, CIP-007 only requires single-factor authentication by using

[942] *See id.*, Requirement R3.

[943] *See id.*, Requirement R3.1.

[944] *See id.*, Requirement R4. The responsible entity also has to implement a process to test new malware signatures before installing them. *See id.*, Requirement R4.1. This is significant, given that incorrect malware signatures have caused significant interferences with system integrity in the past. *Cf. infra* chapter 5.3.3.3 (discussing this issue in the context of product liability and providing numerous examples for it).

[945] *See* NERC, CYBER SECURITY — SYSTEMS SECURITY MANAGEMENT, CIP-007-3, Requirement R5 (2009), *available at* http://www.nerc.com/files/CIP-007-3.pdf.

[946] An audit trail of individual user account access activity has to be maintained for a minimum of 90 days. *See id.*, Requirement R5.1.2.

[947] A responsible entity has to ensure that user accounts are implemented as approved by designated personnel. *See id.*, Requirement R5.1.1. User accounts also have to be reviewed at least annually to verify access privileges are in accordance with CIP-003 Requirement R5 and CIP-004 Requirement R4. *See id.*, Requirement R5.1.3.

[948] *See id.*, Requirement R5.2. Apparently, some SCADA systems are shipped with default accounts the passwords of which may not be changed. *See* Robert McMillan, *Siemens warns users: Don't change passwords after worm attack*, INFOWORLD, July 10, 2010, http://www.infoworld.com/d/security-central/siemens-warns-users-dont-change-passwords-after-worm-attack-915?page=0,0&source=rss_security_central.

passwords which, if technically feasible, (1) have to be at least six characters long, (2) must consist of a combination of alpha, numeric, and "special" characters, and (3) have to be changed at least annually, or more frequently based on risk.[949]

Sixth, organizational processes as well as technical and procedural mechanisms have to be implemented for monitoring security events on all Cyber Assets within an ESP.[950]

Seventh, responsible entities must implement administrative safeguards to address risks associated with the disposal or redeployment of Cyber Assets within the ESPs.[951]

Lastly, responsible entities have to perform, at least annually, a cyber vulnerability assessment of all Cyber Assets within the ESP[952] and have to review and update the documentation specified in CIP-007.[953]

In summary, CIP-007 takes a comprehensive approach to system security. However, it contains three major deficiencies that significantly reduce the standard's effectiveness: First, it does not set any deadlines for installing security updates.[954] CIP-007 only provides a deadline for the evaluation by a responsible entity whether a security update is at all

[949] *See id.*, Requirement R5.3.

[950] *See id.*, Requirement R6.

[951] *See id.*, Requirement R7. In particular, the data storage media has to be erased prior to disposal or redeployment. *See id.*, Requirement R7.1-2.

[952] *See id.*, Requirement R8. The assessment has to include: (1) the documentation of the vulnerability assessment process; (2) a review to verify that only ports and services required for operation of the Cyber Assets within the ESP are enabled; (3) a review of controls for default accounts; and (4) documentation of the results of the assessment, the action plan to remediate or mitigate identified vulnerabilities, and the execution status of that action plan. *See id.*, Requirement R8.1-4.

[953] *See id.*, Requirement R9.

[954] This is particularly significant since the unpatched published vulnerabilities have been identified as the most likely access vector for Industrial Control Systems. *See* IDAHO NAT'L LABORATORY, NSTB ASSESSMENTS SUMMARY REPORT: COMMON INDUSTRIAL CONTROL SYSTEM CYBER SECURITY WEAKNESSES 7 (2010), *available at* http://www.fas.org/sgp/eprint/nstb.pdf.

applicable for a certain system. That deadline is, however, not risk-based but simply set at 30 days from the availability of the update. For critical security updates, this 30-day evaluation period—which would necessarily have to be followed by a testing period—is overly long and not adequate for the risk presented.[955]

The second major deficiency of CIP-007 is that, irrespective of the risk presented, it only requires single-factor authentication based on potentially weak passwords.[956] Based on the level of risk presented, many Critical Cyber Assets would warrant the implementation of two-factor authentication. Furthermore, if passwords are indeed used for single factor authentication, they should be stronger than required by CIP-007: they should be at least eight rather than six characters[957] and should be checked automatically for insufficient complexity.[958]

The third significant deficiency is that CIP-007 explicitly refers to the possibility that a responsible entity may use shared accounts.[959] Shared accounts (also known as group

[955] *Cf.* PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES, VERSION 2.0, at 38 (2010), *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf (stating that "critical security patches" have to be installed "within one month of release"). *Cf. also* Felicia M. Nicastro, *Security Patch Management: The Process, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 185, 196 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (stating that timeframe for the deployment of a security patch should be defined, based on the criticality of the vulnerability and any other relevant factors).

[956] *Cf.* IDAHO NAT'L LABORATORY, NSTB ASSESSMENTS SUMMARY REPORT: COMMON INDUSTRIAL CONTROL SYSTEM CYBER SECURITY WEAKNESSES 58 (2010), *available at* http://www.fas.org/sgp/eprint/nstb.pdf (noting that passwords are often the weakest link in an authentication architecture).

[957] *See id.* at 60 (stating that "8 or more characters" should be used "whenever possible"); Mollie E. Krehnke & David C. Krehnke, *Sensitive or Critical Data Access Controls, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 739, 747 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (stating that passwords should be complex and at least eight characters in length); SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 1085 (4th ed. 2008) (stating that a strong password policy "should dictate that passwords must be at least eight characters").

[958] *See* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 607 (3d ed. 2003) (describing how to automatically enforce a certain level of password strength for UNIX system accounts).

[959] *See* NERC, CYBER SECURITY — SYSTEMS SECURITY MANAGEMENT, CIP-007-3, Requirements R5.1, R5.2, R5.2.2, and R5.2.3 (2009), *available at* http://www.nerc.com/files/CIP-007-3.pdf.

accounts) exist if multiple individuals log into a system using the same account. They are detrimental to security because they eliminate individual accountability[960] and make it radically more difficult to securely assign a new password.[961]

CIP-008 ("Incident Reporting and Response Planning") requires responsible entities to develop and maintain a plan for responding to "Cyber Security Incidents"[962] and to implement that plan whenever a Cyber Security Incident occurs.[963] The incident response plan has to (1) contain procedures to characterize and classify events as reportable Cyber Security Incidents;[964] (2) define roles and responsibilities of incident response teams and document incident handling procedures as well as communication plans;[965] and (3) specify a process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).[966] Furthermore, the incident response plan has to be updated within thirty calendar days of any changes[967] and has to be reviewed and tested at least annually.[968]

[960] *See* Sean M. Price, *Operations Security, in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 633, 638 (Harold F. Tipton ed., 2007); SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 582 (3d ed. 2003).

[961] If multiple individuals have to be informed about a new password, it often has to be communicated in an unencrypted form. If, on the other hand, an account is only used by a single individual, he can change the password himself without any further need to communicate the password.

[962] *See* NERC, GLOSSARY OF TERMS USED IN NERC RELIABILITY STANDARDS 12 (2010), *available at* http://www.nerc.com/page.php?cid=2|20|283 (defining "Cyber Security Incident" as "[a]ny malicious act or suspicious event" that either "[c]ompromises, or was an attempt to compromise, the [ESP] or [PSP] of a Critical Cyber Asset," or, "[d]isrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset").

[963] NERC, CYBER SECURITY — INCIDENT REPORTING AND RESPONSE PLANNING, CIP-008-3, Requirement R1 (2009), *available at* http://www.nerc.com/files/CIP-008-3.pdf.

[964] *See id.*, Requirement R1.1.

[965] *See id.*, Requirement R1.2.

[966] *See id.*, Requirement R1.3. *See also* http://www.esisac.com (last accessed Feb. 10, 2011).

[967] *See id.*, Requirement R1.4.

[968] *See id.*, Requirement R1.5-6. Note that a simple paper drill fulfills the annual testing requirement as well as a full operational exercise. *See id.*

CIP-008 fails to address an issue that is critical for the success of any incident response program: the human resource component. CIP-008 only once refers to "Cyber Security Incident response teams"[969] but does not specify whether such teams are to be formed on a permanent or ad hoc basis. Furthermore, CIP-008 does not establish any requirements regarding the incident response skills of potential team members or their training.[970]

CIP-009 ("Recovery Plans for Critical Cyber Assets") requires that responsible entities create, maintain, and test recovery plans for Critical Cyber Assets.[971] At a minimum, a recovery plan has to specify the event, in response to which it should be activated, define the roles and responsibilities of responders, and describe backup and restore procedures.[972]

A recovery plan has to be reviewed[973] and exercised at least annually.[974] It has to be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident, whereas updates shall be communicated to responsible personnel within thirty calendar days.[975]

[969] *See id.*, Requirement R1.2.

[970] The learning effect of the annually required tests of the incident response plan may also be limited if they are—as permissible under CIP-008 Requirement R1.6—only performed as paper drills. *Cf.* EUGENE E. SCHULTZ & RUSSELL SHUMWAY, INCIDENT RESPONSE: A STRATEGIC GUIDE TO HANDLING SYSTEM AND NETWORK SECURITY BREACHES 103 (2001) (emphasizing the importance of training the incident response team); Marcus K. Rogers, *Legal, Regulations, Compliance and Investigations, in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 683, 699 (Harold F. Tipton ed., 2007) (noting that "[t]o have effective and efficient incident handling, [a] properly staffed and trained response team is also required").

[971] *See* NERC, CYBER SECURITY — RECOVERY PLANS FOR CRITICAL CYBER ASSETS, CIP-009-3 (2009), *available at* http://www.nerc.com/files/CIP-009-3.pdf.

[972] *See id.*, Requirements R1.1, R1.2, R4.

[973] *See id.*, Requirements R1.

[974] *See id.*, Requirements R2 (stating that an exercise can range from a paper drill to a full operational exercise). However, backup media that holds information essential to recovery has to be actually tested on a yearly basis. *See id.*, Requirement R5.

[975] *See id.*, Requirements R3.

Like CIP-008, CIP-009 is rather short and of a general nature. It too, fails to address the human resource component by not mandating any training and only requiring an annual exercise in the form of a paper drill.[976]

In summary, the CIP standards implement a very comprehensive approach to information security.[977] However, the above analysis reveals that they contain the following deficiencies: (1) an overly narrow definition of Critical Cyber Assets (CIP-002); (2) weak authentication in the context of personnel risk assessment, physical access, and electronic access to Cyber Assets (CIP-004, CIP-007, CIP-006); (3) weak accountability by allowing shared accounts (CIP-007); (4) an overly long period for revoking access rights after termination (CIP-004); (5) a Technical Feasibility Exception for authentication of external interactive access to ESPs, and the implementation of an ESP intrusion detection system (CIP-005); (6) no deadline for installing security updates (CIP-007); and (7) no mandatory training for incident response and recovery (CIP-008, CIP-009). Additionally, the CIP standards collectively overstate the significance of perimeter security[978] while not mandating strong host-based security controls

[976] *See id.*, Requirements R2. Depending on the level of risk presented, a simulation test or even a parallel test might be more appropriate than a paper drill (sometimes also referred to as a tabletop exercise or a walk-through test). *See* Carl B. Jackson, *Business Continuity and Disaster Recovery Planning, in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 337, 390 (Harold F. Tipton ed., 2007)*;* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 819 (4th ed. 2008); James S. Mitts, *Testing Business Continuity and Disaster Recovery Plans, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1629, 1631 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007).

[977] *Cf.* DEBRA S. HERRMANN, COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS: MEASURING REGULATORY COMPLIANCE, OPERATIONAL RESILIENCE, AND ROI 323 (2007) (noting that the CIP standards "are probably one of the most comprehensive sets of security standards in existence today").

[978] *See* IDAHO NAT'L LABORATORY, NSTB ASSESSMENTS SUMMARY REPORT: COMMON INDUSTRIAL CONTROL SYSTEM CYBER SECURITY WEAKNESSES 74 (2010), *available at* http://www.fas.org/sgp/eprint/nstb.pdf (summarizing the limitations of security through perimeter defenses). *Cf. also* STEPHEN NORTHCUTT ET AL., INSIDE NETWORK PERIMETER SECURITY 6 (2d ed. 2005) (discussing the importance of implementing additional security controls inside of the network that is protected by perimeter defenses); WILLIAM R. CHESWICK ET AL., FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER 11 (2d ed. 2003) (noting that perimeter security is problematic if the number of hosts within the perimeter is too large); NITESH DHANJANI ET AL., HACKING: THE NEXT GENERATION 25 et seq. (2009) (noting that the flaw with the perimeter-based approach to

(e.g. host-based firewalls).[979] Regrettably, none of these deficiencies will be addressed by the version 4 of the CIP standards, currently awaiting approval by FERC.[980]

Like all reliability standards, the CIP standards are generally to be enforced by NERC[981] which may delegate,[982] subject to approval by FERC,[983] its enforcement authority to Regional Entities.[984] Currently, NERC has delegated its enforcement authority to eight Regional Entities[985] which are also private entities and over which it retains oversight responsibility.[986]

security is that all the insiders are assumed to be fully trustworthy and further discussing how malicious threat agents are able to exploit web application and browser flaws to launch "inside-out" attacks).

[979] Note that the CIP standards do not require the implementation of host-based firewalls *Cf.* NERC, FREQUENTLY ASKED QUESTIONS (FAQS) FOR CYBER SECURITY STANDARDS: CIP-007-1 — CYBER SECURITY — SYSTEMS SECURITY MANAGEMENT 7 (2006), *available at* http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-007-1_FAQs_20090217.pdf (noting that a host-based firewall may be used as a compensating measure if ports and services that cannot be disabled).

[980] Version 4 of the CIP standards is available at http://www.nerc.com/page.php?cid=2|20 (last accessed Feb. 10, 2011).

[981] Federal Power Act § 215(e)(1), 16 U.S.C. § 824o(e)(1) (stating that the ERO may impose a penalty for a violation of a FERC-approved reliability standard "if the ERO, after notice and an opportunity for a hearing (A) finds that the user or owner or operator has violated a reliability standard approved by the Commission under subsection (d) of this section; and (B) files notice and the record of the proceeding with the Commission").

[982] *See* 18 C.F.R. § 39.8(a) (implementing Federal Power Act § 215(e)(4) which required FERC to "issue regulations authorizing the ERO to enter into an agreement to delegate authority to a regional entity for the purpose of proposing reliability standards to the ERO and enforcing reliability standards").

[983] *See* 18 C.F.R. § 39.8(b) (stating that "[a]fter notice and opportunity for comment, the Commission may approve a delegation agreement. A delegation agreement shall not be effective until it is approved by the Commission.").

[984] *See* Federal Power Act § 215(e)(4), 16 U.S.C. § 824o(e)(4) (stating that a delegation to a Regional Entity may only be performed if (A) the regional entity is governed by (i) an independent board, (ii) a balanced stakeholder board, or (iii) a combination of both; (B) it satisfies the requirements for an ERO (§ 215(c)(1) and (2)); and (C) the delegation agreement promotes effective and efficient administration of bulk-power system reliability).

[985] These are: the Florida Reliability Coordinating Council (FRCC), the Midwest Reliability Organization (MRO), the Northeast Power Coordinating Council (NPCC), the ReliabilityFirst Corporation (RFC), the SERC Reliability Corporation (SERC), the Southwest Power Pool Regional Entity (SPP RE), the Texas Reliability Entity (TRE), and the Western Electricity Coordinating Council (WECC). *See* http://www.nerc.com/page.php?cid=3|23 (last accessed Feb. 10, 2011). The delegation agreements are available at http://www.nerc.com/page.php?cid=1|9|119|181 (last accessed Feb. 10, 2011). *Cf.* JACK CASAZZA & FRANK DELEA, UNDERSTANDING ELECTRIC POWER SYSTEMS: AN OVERVIEW OF TECHNOLOGY, THE MARKETPLACE, AND GOVERNMENT REGULATION 168 (2d ed. 2010) (depicting the location of the Regional Entities).

[986] *Cf.* Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards, 71 Fed. Reg. 8,662, 8,666 (Feb. 17,

In addition to these Regional Entities, FERC itself may also enforce the reliability standards.[987] Penalties assessed by NERC or one of the Regional Entities are subject to review by FERC.[988]

As of February, 2011 there have been 4 enforcement actions under CIP-002, 6 under CIP-003, 19 under CIP-004, 1 under CIP-005, 2 under CIP-006, 4 under CIP-007, 3 under CIP-008, and 3 under CIP-009.[989]

4.3.3. The EU eSignature Directive

Parliament and Council Directive 1999/93[990] (hereinafter *eSignature Directive*) establishes a legal framework for electronic signatures and certification services. While attempting to be neutral with regard to the technology used,[991] the eSignature Directive is clearly focused on asymmetric cryptography[992] and, more specifically, a Public Key Infrastructure (PKI).[993] This is understandable, given that asymmetric cryptography is currently the only technological

2006) (stating that "[t]he ERO will retain oversight responsibility for enforcement authority that is delegated to a Regional Entity").

[987] *See* Federal Power Act § 215(e)(3), 16 U.S.C. § 824o(e)(3) (stating that FERC may, "[o]n its own motion or upon complaint, […] order compliance with a reliability standard and may impose a penalty").

[988] *See* Federal Power Act § 215(e)(2), 16 U.S.C. § 824o(e)(2); 18 C.F.R. § 39.7(e)(1).

[989] *See* http://www.nerc.com/filez/enforcement/index.html (last accessed Feb. 10, 2011).

[990] 2000 O.J. (L 13) 12 (EC) as amended by Parliament and Council Regulation No. 1137/2008, 2008 O.J. (L 311) 1 (EC).

[991] *Cf.* eSignature Directive recital 8 (stating that "[r]apid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically").

[992] Asymmetric cryptography refers to a branch of cryptography that is based on using one key for encryption and using a different but complementary key for decryption. *Cf.* Javek Ikbal, *An Introduction to Cryptography, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1121, 1129 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007).

[993] *Cf.* NIELS FERGUSON ET AL., CRYPTOGRAPHY ENGINEERING: DESIGN PRINCIPLES AND PRACTICAL APPLICATIONS 275 (2010) (providing a brief introduction into the architecture of a PKI).

solution available to implement electronic signatures that provide integrity, authenticity, and non-repudiation[994] of signed information.[995]

Most significantly, the eSignature Directive states that legal requirements of a signature are satisfied by an electronic signature in the same manner as a handwritten signature[996] if the electronic signature (1) provides authenticity, non-repudiation, and integrity (i.e. is an "advanced electronic signature");[997] (2) is created by a device that meets certain legal requirements (a "secure-signature-creation device");[998] and (3) is based on a "qualified certificate."[999]

It is of relevance here that the Directive requires entities that issue "qualified certificates" to fulfill the requirements set out it appendix II of the eSignature Directive.[1000] Such entities are referred to by the Directive as "certification-service-providers."[1001] From a technological

[994] *Cf. supra* chapter 2.1 (discussing and providing further references for the information security properties of integrity, authenticity, and non-repudiation).

[995] *Cf. Commission Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures*, at 4, COM (2006) 120 final (Mar. 15, 2006) (stating that "[t]he Directive is technology neutral but in practice, [the definition of 'advanced electronic signature'] refers mainly to electronic signatures based on a public key infrastructure (PKI)").

[996] *See* eSignature Directive art. 5(1).

[997] *See* eSignature Directive art. 2(2) (defining "advanced electronic signature" as "an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable"). This term is to be differentiated from other "electronic signatures" as defined by eSignature Directive art. 2(1) which do not provide authenticity (*cf.* art. 2(2)(a) and (b)), non-repudiation (*cf.* art. 2(2)(c)), or integrity (*cf.* art. 2(2)(d)).

[998] *See* eSignature Directive art. 2(6) (defining "secure-signature-creation device" as "a signature-creation device which meets the requirements laid down in Annex III"). These requirements are discussed *infra* in chapter 4.5.3.

[999] *See* eSignature Directive art. 2(10) (defining "qualified certificate" as "a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II").

[1000] *See* eSignature Directive annex II (entitled "Requirements for certification-service-providers issuing qualified certificates").

[1001] *See* eSignature Directive art. 2(11) (defining a "certification-service-provider" as "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures").

perspective of a PKI, they perform the role of a Certificate Authority and a Registration Authority.[1002] Certification-service-providers have to implement the following security controls:

First, they have to implement a number of controls that are essential for any Certificate Authority: (1) ensuring the operation of a "prompt and secure directory and a secure and immediate revocation service";[1003] (2) ensuring that the date and time when a certificate is issued or revoked can be determined precisely;[1004] (3) taking measures against forgery of certificates, and, in cases where certification-service-providers generate private keys ("signature-creation data"),[1005] guarantee confidentiality during the generation process;[1006] and (4) not storing or copying private keys of the person to whom the key management services are provided.[1007]

[1002] *Cf.* CARLISLE ADAMS & STEVE LLOYD, UNDERSTANDING PKI: CONCEPTS, STANDARDS, AND DEPLOYMENT CONSIDERATIONS 85 et seq. (2d ed. 2003) (describing the respective roles of a Certificate Authority and a Registration Authority).

[1003] *See* eSignature Directive annex II.b. The revocation service is of particular importance because it allows a certificate that has been compromised to be revoked, thereby letting third parties know that signatures that have been created using this certificate cannot be trusted. *Cf.* NIELS FERGUSON ET AL., CRYPTOGRAPHY ENGINEERING: DESIGN PRINCIPLES AND PRACTICAL APPLICATIONS 289 (2010) (discussing the challenges of certificate revocation).

[1004] *See* eSignature Directive annex II.c.

[1005] *See* eSignature Directive art. 2(4) (defining "signature-creation data" as "unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature").

[1006] *See* eSignature Directive annex II.g.

[1007] *See* eSignature Directive annex II.j.

Second, they have to fulfill their role as a Registration Authority by authenticating[1008] "by appropriate means in accordance with national law" any person to which a certificate is issued.[1009]

Third, certification-service-providers have to implement administrative security controls: (1) employing personnel, in particular at managerial level, who possess the expert knowledge, experience, and qualifications "necessary for the services provided,"[1010] (2) applying administrative and management procedures which are "adequate and correspond to recognized standards."[1011]

Fourth, they have to use "trustworthy systems and products."[1012] The eSignature Directive grants the Commission the power to publish references to generally recognized standards, the compliance with which creates the presumption that the systems and products are indeed trustworthy.[1013] In 2003, the Commission used this power to create a presumption of

[1008] *Cf.* chapter 4.1.10.1 (discussing the important difference between authentication and identification in the context of impersonation fraud).

[1009] *See* eSignature Directive annex II.c.

[1010] *See* eSignature Directive annex II.e.

[1011] *See id.* Note that the eSignature Directive does not provide any guidance to determine which measures are "adequate"; it also does not require certification-service providers to obtain any certifications with regard to the compliance with "recognized standards."

[1012] *See* eSignature Directive annex II.f, l.

[1013] *See* eSignature Directive art. 3(5).

trustworthiness for all products that comply with CWA 14167-1:2003[1014] and CWA 14167-2:2002.[1015]

4.3.4. Comparative Assessment

4.3.4.1. Requiring "Appropriate" v. Specific Safeguards

As previously discussed in the context of mandatory security controls for personal information controllers, it is one of the most significant questions whether a regulatory policy requires the implementation of certain specific safeguards or the implementation of "appropriate" safeguards.[1016] In this regard, the three regulatory regimes discussed above, show very significant differences.

The Telecoms Framework Directive requires the implementation of "appropriate" safeguards to "appropriately manage the risks posed to" the availability of public communications networks and services.[1017] For a provider or a regulatory authority to verify compliance, it is therefore necessary to perform a risk assessment. However, the Telecoms Framework Directive does not mandate that any specific risk assessment method be used, leading to a number of very significant problems described in detail *supra* in chapter 4.1.10.4.[1018] Most

[1014] *See* EUROPEAN COMM. FOR STANDARDIZATION [CEN], SECURITY REQUIREMENTS FOR TRUSTWORTHY SYSTEMS MANAGING CERTIFICATES FOR ELECTRONIC SIGNATURES –PART 1: SYSTEM SECURITY REQUIREMENTS, CEN WORKSHOP AGREEMENT CWA 14167-1 (2003), *available at* ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-01-2003-Jun.pdf.

[1015] *See* Commission Decision 2003/511, 2003 O.J. (L 175) 45, 46 (EC). *See* CEN, SECURITY REQUIREMENTS FOR TRUSTWORTHY SYSTEMS MANAGING CERTIFICATES FOR ELECTRONIC SIGNATURES – PART 2: CRYPTOGRAPHIC MODULE FOR CSP SIGNING OPERATIONS – PROTECTION PROFILE (MCSO-PP), CEN WORKSHOP AGREEMENT CWA 14167-2 (2002), *available at* http://www.interlex.it/testi/pdf/cwa14167-2.pdf.

[1016] *See supra* chapter 4.1.10.4.

[1017] Telecoms Framework Directive art. 13a(1).

[1018] One of the problems discussed in chapter 4.1.10.4 is that of "best practices" being used irrespective of whether they have any proven track record of actually mitigating risks. This particular problem might not be significantly, it is entirely unclear how the risk of unavailability is to be quantified, thus making it difficult to enforce the requirement that safeguards have to be implemented that "appropriately manage the risks."[1019]

In stark contrast to the Telecoms Framework Directive, the NERC standards establish very specific requirements that do not depend on any measurement of risk. On the one hand, this eliminates the problem of having to perform risk assessments during the compliance process as well as the enforcement process. However, it does not eliminate the challenges of risk assessment as such because it merely shifts the burden of conducting the assessment from the regulated entity (and the enforcement body) to the regulator.[1020] With regard to the NERC standards, the question therefore is how appropriately the regulatory requirements address information security risks. In chapter 4.3.2 it has been shown that the NERC standards contain a number of very basic deficiencies, ultimately rendering them insufficient to address the information security risks to which the bulk-power system and SCADA systems in particular are exposed to. Furthermore, the deficiencies of the NERC standards cannot be compensated by stronger enforcement, possibly by FERC, since the standards are inflexible in the sense that they establish specific requirements, irrespective of the magnitude of risk presented in a particular case.[1021]

very significant in the context of public communications services and networks because indeed few "best practices" are currently defined. *See* ENISA, NETWORK PROVIDER MEASURES: RESILIENCE OF COMMUNICATION NETWORKS 42 (2008), *available at* http://www.enisa.europa.eu/act/res/providers-measures/files/network-provider-measures/at_download/fullReport (stating that best practices are "insufficiently defined").

[1019] Telecoms Framework Directive art. 13a(1).

[1020] *Cf. supra* chapter 4.1.10.4.

[1021] Of course, responsible entities would be well advised to use the CIP standards only as a set of minimum requirements. Legally, however, they are not required to go beyond the CIP standards. *Cf.* DEBRA S. HERRMANN, COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS: MEASURING REGULATORY COMPLIANCE, OPERATIONAL

The NERC standards therefore demonstrate that implementing a policy that is based on specific safeguard requirements, irrespective of the magnitude of risk may also lead to ineffective information security regulation.

The eSignature Directive covers a middle ground between the Telecoms Framework Directive and the NERC standards. While establishing specific security requirements, it describes these requirements in more general terms, allowing a more flexible, risk-based enforcement. One security requirement of the eSignature Directive is of particular interest: certification-service-providers have to use "trustworthy systems and products"[1022] whereby the adherence to Commission-approved technical standards creates a *presumption of compliance*.[1023] On the one hand, this approach allows regulated entities to comply with this regulatory requirement simply by purchasing systems and products that have been certified against the approved technical standards by a third party testing organization. On the other hand, regulated entities are not confined to a particular technical standard and may also demonstrate compliance by other means. In the EU, this regulatory approach has been termed the "New Approach."[1024]

RESILIENCE, AND ROI 309 (2007) (noting that "[r]eality" (but not compliance with the CIP standards) "may necessitate that a given organization deploy more robust security practices").

[1022] *See* eSignature Directive annex II.f, l.

[1023] *See* eSignature Directive art. 3(5).

[1024] The "New Approach" was launched by Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards, 1985 O.J. (C 136) 1. Its four fundamental principles are: (1) legislative harmonization is to be limited to "essential safety requirements"; (2) the task of drawing up the technical specifications is entrusted to the European standards bodies; (3) these technical specifications remain voluntary in nature; and (4) national authorities are obliged to recognize that products manufactured in conformity with harmonized standards are presumed to conform to the "essential requirements" established by the Directive. *See id.*, annex II. Currently, there are at least 45 directives which are based on the "New Approach." *See* http://ec.europa.eu/enterprise/policies/european-standards/documents/harmonised-standards-legislation/list-references/ (last accessed Feb. 10, 2011). *Cf. also* CHRISTIAN JOERGES ET AL., THE LAW'S PROBLEMS WITH THE INVOLVEMENT OF NON-GOVERNMENTAL ACTORS IN EUROPE'S LEGISLATIVE PROCESSES: THE CASE OF STANDARDISATION UNDER THE 'NEW APPROACH,' EUI WORKING PAPER LAW NO. 99/9 (1999), *available at* http://cadmus.eui.eu/bitstream/handle/1814/154/law99_9.pdf?sequence=1.

While it potentially provides advantages over traditional regulation,[1025] its usefulness is also limited to product categories that are (1) not too complex and (2) sufficiently homogeneous to allow common requirements to be defined.[1026] However, most IT products, in particular larger software products, are not only too heterogeneous but also too complex[1027] to allow meaningful certification within a reasonable timeframe.[1028] Cryptographic devices are an exception since they typically only have to perform a small set of clearly defined functions that can be specified and certified rather easily.

Furthermore, the effectiveness of a regulatory regime that follows the "New Approach" is highly dependent on the quality of the standards that create the presumption of compliance. The eSignature Directive serves as a particularly bad example in this regard since CWA

[1025] *See Commission Communication on Standardization in the European Economy (Follow-up to the Commission Green Paper of October 1990)*, at 31, COM (91) 521 final (Dec. 16, 1991) (stating the advantages of the "New Approach" as follows: (1) standardization is a highly transparent process in which all interested parties may be involved; (2) it combines the advantages of democracy with the ability to reflect the technological state-of-the-art; (3) standards can be easily modified to reflect technological development; (4) reference to standardization in legislation means that most of the costs of production of technical specifications are transferred from the public to the private sector; (5) standardization may be more efficient than technical regulation, in so far as it will better reflect technical reality in the market).

[1026] Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards, 1985 O.J. (C 136) 1, 8 (stating that "[s]ince the approach calls for the 'essential requirements' to be harmonized and made mandatory by Directives […], the [new approach] will be appropriate only where it is genuinely possible to distinguish between 'essential requirements' and 'manufacturing specifications'").

[1027] *Cf. supra* chapter 2.3.3 (discussing the reasons for the continuously increasing complexity of software).

[1028] The evaluation and certification of IT products is typically performed in accordance with ISO/IEC 15408 (commonly referred to as *Common Criteria* or *CC*). *See* Debra S. Herrmann, *The Common Criteria for IT Security Evaluation*, *in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1487 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (providing an introduction into the CC). The CC provides seven Evaluation Assurance Levels (EALs), ranging from EAL1 (the most basic level) to EAL7 (the most stringent level). Despite the fact that commercial software is typically, at most, certified at EAL4—which does not include a review of the source code—CC evaluations are very expensive and time-consuming. *Cf.* ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 529 (2d ed. 2008). Most significantly, a CC certification only speaks to the question of whether a product complies with a certain set of implementation-independent security requirements (referred to as a Protection Profile) which are typically drafted by the manufacturer. In an effort to shorten the certification process, manufacturers often include unrealistic assumptions about the product's environment in their Protection Profiles. *See* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 32 (2007) (noting that this makes it difficult to translate EAL ratings into the real world).

14167-2—which is supposed to create a presumption of compliance with annex II(f) of the eSignature Directive—for certain requirements refers to a standard that has not been approved and can therefore not be used in practice to certify any systems or products.[1029] The effective criteria used by Member States in practice therefore differ significantly.[1030]

4.3.4.2. Direct Government Regulation vs. Audited Self-Regulation

The Telecoms Framework Directive and the eSignature Directive implement traditional approaches based on direct government regulation.[1031] The Energy Policy Act of 2005, however, adopts a regulatory approach best described as "audited self-regulation."[1032]

In contrast to direct government regulation (and voluntary self-regulation), audited self-regulation involves the formal delegation of regulatory powers to a private actor, subject to government oversight. This private actor—NERC in the case of the Energy Policy Act of 2005—can be described as a "self-regulatory organization."[1033]

[1029] As mentioned in the preceding footnote, Common Criteria certifications are necessarily performed against certain Protection Profiles. However, CWA 14167-2 refers to a Protection Profile that is not been certified itself and therefore cannot be used for a certification. *See* SEALED ET AL., STUDY ON CROSS-BORDER INTEROPERABILITY OF ESIGNATURES (CROBIES), NOTE ON THE "ALGO PAPER" ISSUE 5 n.11 (2010), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.3.pdf. *Cf. also* RUNDFUNK UND TELEKOM REGULIERUNGS-GMBH, 4 JAHRE SIGNATURGESETZ [4 YEARS SIGNATURE ACT] 109 (2004), *available at* http://www.signatur.rtr.at/repository/rtr-report-20040116-de.pdf.

[1030] *See* SEALED ET AL., STUDY ON CROSS-BORDER INTEROPERABILITY OF ESIGNATURES (CROBIES), COMMON SUPERVISION MODEL OF PRACTICES OF CERTIFICATION SERVICE PROVIDERS ISSUING QUALIFIED CERTIFICATES 21 (2010), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd1.pdf.

[1031] Regulatory aspects of the "New Approach" implemented by the eSignature Directive are discussed in the preceding chapter.

[1032] Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 650 (2000) (generally describing "audited self-regulation" as instances in which Congress officially "deputizes" private actors as regulators, by formally delegating to them the authority to set and implement standards, subject to agency oversight). *Cf. also* Jody Freeman, *Private Parties, Public Functions and the New Administrative Law*, 52 ADMIN. L. REV. 813, 834 (2000) (also using the term "mandatory self-regulation").

[1033] The term "self-regulatory organization" was first defined in Security Exchange Act of 1934, § 3(26), 15 U.S.C.A. § 78c(26) (defining "self-regulatory organization" as "any national securities exchange, registered

Under the Energy Policy Act of 2005, the oversight responsibility is exercised by FERC which retains the power to approve or reject reliability standards drafted by the ERO,[1034] may order the ERO to draft or modify certain standards,[1035] and may even assess penalties or suspend or rescind the ERO's authority if it does not comply with an order.[1036]

While traditional regulatory agencies may be subject to capture by the industries they regulate,[1037] a self-regulatory organization is, by definition, captured by the interests of the regulated industry. The NERC standards perfectly demonstrate this danger: as discussed *supra*, they contain a number of very significant deficiencies ultimately rendering them fundamentally inadequate.[1038]

However, pragmatically speaking, audited self-regulation may nevertheless be an appropriate regulatory approach—as least at an interim measure—if direct government regulation is politically infeasible.

securities association, or registered clearing agency, or […] the Municipal Securities Rulemaking Board established by section 78o-4 of this title"). NERC has sought the status of a "self-regulatory organization" at least since 2001. *See The Electric Supply and Transmission Act of 2001: Hearing on H.R. 3406 Before the H. Comm. on Energy and Commerce*, 107th Cong. 153 (2001) (statement of Michel R. Gent, President and Chief Executive Officer, North American Electric Reliability Council: "NERC and a substantial majority of other industry participants believe that the best way to [ensure the reliability of the electric transmission system] is through an independent, industry self-regulatory organization with FERC oversight, modeled after the securities industry, where the Securities and Exchange Commission has oversight of several self-regulatory organizations").

[1034] *See* Federal Power Act § 215(d)(2), 16 U.S.C. § 824o(d)(2).

[1035] *See* Federal Power Act § 215(d)(5), 16 U.S.C. § 824o(d)(5).

[1036] *See* Federal Power Act § 215(e)(5), 16 U.S.C. § 824o(e)(5).

[1037] For classic works on agency capture by regulated industries, see generally Richard A. Posner, *Theories of Economic Regulation*, 5 BELL J. ECON. & MGMT. SCI. 335, 341 (1974); George J. Stigler, *The Theory of Economic Regulation*, 2 BELL J. ECON. & MGMT. SCI. 3 (1971).

[1038] *See supra* chapter 4.3.2.

4.4. Mandatory Security Controls for Government Authorities

4.4.1. Federal Information Security Management Act

The Federal Information Security Management Act of 2002[1039] (hereinafter *FISMA*) was enacted as Title III of the E-Government Act of 2002.[1040] It generally requires each federal agency,[1041] under the oversight of the Director of the Office of Management and Budget (OMB),[1042] to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[1043]

[1039] Pub. L. No. 107–347, Title III, §§ 301-305, 116 Stat. 2946 (2002) (codified at 44 U.S.C. §§ 3541-49; 44 U.S.C. § 3501 note; and 40 U.S.C. § 11331).

[1040] Pub. L. No. 107–347, 116 Stat. 2899 (2002).

[1041] *See* 44 U.S.C. § 3542(a) (2010) (defining, by way of reference to 44 U.S.C. § 3502(1), the term "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include (A) the Government Accountability Office; (B) Federal Election Commission; (C) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities").

[1042] *See* 44 U.S.C. § 3543 (outlining the responsibilities of the "Director"). *Cf.* 44 U.S.C. § 3542(a) (defining, by way of reference to 44 U.S.C. § 3502(4), the term "Director" as "the Director of the Office of Management and Budget"). Note that the Director's authority over systems operated by or on behalf of the Department of Defense or the Central Intelligence Agency is, to a significant extent, delegated by the statute to the Secretary of Defense and the Director of Central Intelligence, respectively. *See* 44 U.S.C. § 3543(c). The authorities of the Director also do not apply to national security systems. 44 U.S.C. § 3543(b). *Cf.* 44 U.S.C. § 3542(b)(2)(A) (defining the term "national security system").

[1043] *See* 44 U.S.C. § 3544(b).

At the outset, it should be emphasized that FISMA is the only federal law—indeed the only regulatory regime in the U.S. and the EU—that defines "information security" as fully encompassing information confidentiality, integrity, and availability.[1044]

As regards FISMA's personal scope of application, it is also noteworthy that FISMA, albeit not directly applying to contractors, requires federal agencies to ensure that their contractors are in compliance with FISMA.[1045]

Specifically, a federal agency's information security program has to include the following elements:

First, it has to include a periodic risk assessment.[1046] However, FISMA does not require that any particular risk assessment method be used. This is a significant shortcoming since many methods commonly used today are indeed inadequate for objectively measuring risk.[1047] Making things worse, a (non-obligatory) guidance published by the National Institute of Standards and Technology (NIST) advocates the use of a scoring method based on a

[1044] *See* 44 U.S.C. § 3542(b)(1) (defining "information security" broadly as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information").

[1045] *See* 44 U.S.C. § 3544(a)(1)(A)(ii) (describing federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency"); 44 U.S.C. § 3544(b) (requiring an agency's security program to cover "information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source"). *Cf. also* OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-10-15, FY 2010 REPORTING INSTRUCTIONS FOR THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT AND AGENCY PRIVACY MANAGEMENT 13 (2010) (stating that "each agency must ensure their contractors are abiding by FISMA requirements").

[1046] *See* 44 U.S.C. § 3544(b)(1).

[1047] *See supra* chapter 4.1.10.4 (discussing the shortcomings of many commonly used risk assessment methods).

qualitative high/medium/low evaluation of likelihood and impact,[1048] which necessarily suffers from range compression, unnecessary ambiguity, and a general lack of objective and verifiable results.[1049]

Second, the security program has to include risk-based cost-effective policies and procedures that, *inter alia*, ensure compliance with information security standards that are drafted by NIST and promulgated by the Directory of the OMB under 40 U.S.C. § 11331. The most significant of these standards are Federal Information Processing Standard (FIPS) 199[1050] and FIPS 200,[1051] which in combination establish a set of minimum security controls for federal information systems: FIPS 199 requires that information systems be assigned impact scores (low, moderate, or high) with regard to the confidentiality, integrity, and availability of the information that resides on these systems.[1052] FIPS 200 provides that the highest impact level assigned to any of the three aspects of information security is to be used as the overall impact

[1048] *See* NIST, RISK MANAGEMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS, SPECIAL PUBLICATION 800-30, at 25 (2002), *available at* http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[1049] *Cf.* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 73 (2009) (specifically criticizing NIST's Special Publication 800-30 for its use of ineffective risk assessment methods). *Cf. also supra* chapter 4.1.10.4 (discussing the shortcomings of scoring methods).

[1050] NIST, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 199 (2004), *available at* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[1051] NIST, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 200 (2006), *available at* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf. A full list of mandatory FISMA standards is available at http://csrc.nist.gov/publications/PubsFIPS.html (last accessed Feb. 10, 2011).

[1052] The following guidelines are not obligatory but are supposed to guide the assignment of impact levels: NIST, VOLUME I: GUIDE FOR MAPPING TYPES OF INFORMATION AND INFORMATION SYSTEMS TO SECURITY CATEGORIES, SPECIAL PUBLICATION 800-60, VOLUME I, REVISION 1 (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf; NIST, VOLUME II: APPENDICES TO GUIDE FOR MAPPING TYPES OF INFORMATION AND INFORMATION SYSTEMS TO SECURITY CATEGORIES, NIST SPECIAL PUBLICATION 800-60, VOLUME II, REVISION 1 (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf.

level of the information system[1053] and that, based on that impact level, a different set of minimum security controls (referred to as a *baseline*) has to be selected.[1054] For a list of the actual security controls to be implemented for low-impact, moderate-impact, and high-impact information systems, FIPS 200 refers to NIST Special Publication 800-53[1055] which provides a detailed list of administrative, technical, and physical security controls. However, since an agency's policies and procedures have to be risk-based,[1056] additional security controls are likely to be necessary to achieve compliance.

An agency's information security program further has to include (1) "subordinate plans" for providing adequate information security;[1057] (2) security awareness training for users of information systems (including contractors);[1058] (3) at least annual testing and evaluation of the agency's policies, procedures, and practices (including all information systems' security controls);[1059] (4) a process for planning, implementing, evaluating, and documenting remedial action to address any identified deficiencies in the agency's policies, procedures, and

[1053] NIST, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 200, at 2 (2006), *available at* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf. For example, if the information that resides on a system has a confidentiality impact level of low, an integrity impact level of low, and an availability impact level of high, the overall system impact level is high. *Cf. id.* (referring to this form of scoring as a "high water mark concept").

[1054] *See id.* at 4.

[1055] *See* NIST, RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, NIST SPECIAL PUBLICATION 800-53 REVISION 3, at 66 et seq. (2009), *available at* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[1056] *See* 44 U.S.C. § 3544(b)(2)(A).

[1057] *See* 44 U.S.C. § 3544(b)(3).

[1058] *See* 44 U.S.C. § 3544(b)(4).

[1059] *See* 44 U.S.C. § 3544(b)(5).

practices;[1060] (5) procedures for detecting, reporting, and responding to security incidents;[1061] and (6) plans and procedures to ensure continuity of operations.[1062]

Despite the use of inadequate risk assessment methods, the security requirements outlined above could significantly mitigate the information security risks federal agencies are facing. However, due to the nature of its mechanisms of compliance monitoring, FISMA is often rightly criticized as a "paperwork exercise"[1063]: FISMA requires each agency to annually issue a report to the Director of the OMB and to Congress[1064] on the adequacy and effectiveness of its policies, procedures, and practices, and compliance with FISMA's requirements.[1065] Furthermore, each agency is obligated to have its information security program independently evaluated annually[1066] and the evaluation results are to be reported to the Director of the OMB.[1067] Until 2010, the Director of the OMB required that all reports use certain metrics and reporting templates[1068] that indeed primarily measured to what extent the

[1060] *See* 44 U.S.C. § 3544(b)(6).

[1061] *See* 44 U.S.C. § 3544(b)(7).

[1062] *See* 44 U.S.C. § 3544(b)(8).

[1063] *See* CENTER FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 69 (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (stating that "[t]o some in government and industry, FISMA has become a paperwork exercise rather than an effective measure of network security"). *Cf.* Daniel M. White, Note, *The Federal Information Security Management Act of 2002: A Potemkin Village*, 79 FORDHAM L. REV. 369, 380 (2010) (providing further references for this assertion).

[1064] An agency has to report to the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General (the director of the Government Accountability Office). *See* 44 U.S.C. § 3544(c)(1).

[1065] 44 U.S.C. § 3544(c)(1).

[1066] The evaluation has to be performed by the agency's Inspector General or by an independent external auditor. *See* 44 U.S.C. § 3545(b).

[1067] 44 U.S.C. § 3545(e).

[1068] See the attachments "CIO Questions" and "IG Questions" to OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-09-29, FY 2009 REPORTING INSTRUCTIONS FOR THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT AND AGENCY PRIVACY MANAGEMENT (2009) *available* documentation of an agency's policies, procedures, and practices complied with FISMA, rather than measuring the extent of compliance of actual procedures and practices.[1069] In particular, these metrics and reporting templates put a strong emphasis on the certification and accreditation (C&A)[1070] of information systems which has been described as a "paperwork nightmare."[1071] The fact that many agencies received, in particular at the beginning, very bad

at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/cio_questions.pdf and http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/ig_questions.pdf.

[1069] *See Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?: Hearing Before the Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the S. Comm. on Homeland Security and Governmental Affairs*, 110th Cong. 8, 9 (2008) (statement of Tim Bennett, President of the Cyber Security Industry Alliance: "FISMA grades reflect compliance with mandated processes. They do not, in my view, measure how much these processes have actually increased information security. In particular, the selection of information security controls is subjective and, thus, not consistent across Federal agencies. Agencies determine on their own what level of risk is acceptable for a given system. They can then implement the corresponding controls, certify and accredit them, and thus be compliant and receive a high grade, regardless of the level of risk they have deemed acceptable."); William Jackson, *FISMA's effectiveness questioned*, GOV'T COMPUTER NEWS, Mar. 18, 2007, http://gcn.com/Articles/2007/03/18/FISMAs-effectiveness-questioned.aspx?Page=1 (quoting Alan Paller, director of research at the SANS Institute: "What we measure now is, 'Do you have a plan?' Not whether the plan actually improves security."); WM. ARTHUR CONKLIN, WHY FISMA FALLS SHORT: THE NEED FOR SECURITY METRICS 8 (SECOND ANNUAL WORKSHOP ON INFORMATION SECURITY AND PRIVACY, 2007), http://www.tech.uh.edu/cae-dc/documents/WISP%202007%20FISMA%20metrics%20paper%20final.pdf (stating that FISMA metrics "do not directly assess aspects of operational security"); DEBRA S. HERRMANN, COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS: MEASURING REGULATORY COMPLIANCE, OPERATIONAL RESILIENCE, AND ROI 285 (2007) (stating that the metrics to be used by Inspectors General "lack an overall assessment of the agency's security engineering life cycle and practices. They also do not evaluate personnel resources."); William Jackson, *Effective IT security starts with risk analysis, former GAO CTO says*, GOV'T COMPUTER NEWS, June 19, 2009, http://gcn.com/Articles/2009/06/15/Interview-Keith-Rhodes-IT-security.aspx?sc_lang=en&Page=2 (quoting Keith Rhodes, former CTO at the Government Accountability Office: "It's not that FISMA hasn't helped or that it needs to be changed. It's a function of the information collection and the oversight associated with it, which needs to be strong. It needs to not be viewed as a paper exercise or allowed to be used as a paper exercise."); Dan Verton, *Survey Finds Digital Divide Among Federal CISOs*, COMPUTERWORLD, Nov. 22, 2004, http://www.computerworld.com/s/article/print/97763/Survey_finds_digital_divide_among_federal_CISOs (quoting John Pescatore, Gartner Inc.: FISMA is "a big paperwork exercise").

[1070] In this context, "certification" can be defined as "the process by which the effectiveness of [an information system's] security controls is assessed" while accreditation is "the management decisions (based on that assessment) to permit an information system to operated at its current security posture." *See* PATRICK D. HOWARD, BUILDING AND IMPLEMENTING A SECURITY CERTIFICATION AND ACCREDITATION PROGRAM: OFFICIAL (ISC)² GUIDE TO THE CAP CBK, at xix (2006).

[1071] LAURA TAYLOR, FISMA CERTIFICATION & ACCREDITATION HANDBOOK 8 (2007) (stating that certification and accreditation "is essentially a documentation and paperwork nightmare").

FISMA scores[1072] therefore primarily indicates that their documentation was not FISMA-compliant. It does not provide a good indication as to the real security posture of federal agencies.[1073] By diverting resources to the documentation rather than implementation[1074] of security controls, FISMA's reporting requirements in place until 2010 may actually have done more harm than good.[1075]

Recognizing these deficiencies, the OMB, by issuing OMB Memorandum M-10-15 in April 2010,[1076] drastically changed the way federal agencies have to fulfill their reporting requirements under FISMA. The memorandum acknowledges that "metrics are a policy

[1072] The overall grade of federal agencies has been a D+ in 2005, a C- in 2006, and a C in 2007. *See* Patience Wait, *Federal government earns a collective D+ on FISMA scorecard*, GOV'T COMPUTER NEWS, Mar. 16, 2006, http://gcn.com/articles/2006/03/16/federal-government-earns-a-collective-d-on-fisma-scorecard.aspx; Frank Washkuch, *Is FISMA fixable?*, SC MAGAZINE, Sept. 1, 2007, http://www.scmagazineus.com/is-fisma-fixable/article/35617/ (stating that the government's overall grade rose to a C– for fiscal year 2006); Jim Carr, *Federal agencies' FISMA grade up slightly*, SC MAGAZINE, May 20, 2008, http://www.scmagazineus.com/federal-agencies-fisma-grade-up-slightly/article/110375/ (stating that the government's overall grade rose to a C for fiscal year 2007). The OMB reports for the fiscal years of 2008 and 2009 show further improvement. *See* OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, FISCAL YEAR 2008 REPORT TO CONGRESS ON IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002, at 6-7 (2009), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/reports/fy2008_fisma.pdf; OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, FISCAL YEAR 2009 REPORT TO CONGRESS ON THE IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002, at 28 (2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf (providing a comparison between all fiscal years from 2002 to 2009).

[1073] *Cf.* Ben Bain, *Improved FISMA scores don't add up to better security, auditor says*, FEDERAL COMPUTER WEEK, June 29, 2009 (stating that the current choice of metrics is partly to blame for the fact that agencies are reporting improved compliance with security requirements even while government investigators continue to find security gaps).

[1074] *Cf.* DEBRA S. HERRMANN, COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS: MEASURING REGULATORY COMPLIANCE, OPERATIONAL RESILIENCE, AND ROI 292 (2007) (noting that, on average, an agency spends $40,000 to perform C&A for a single information system).

[1075] *Cf.* J. Nicholas Hoover, *White House Updates Cybersecurity Orders*, INFORMATIONWEEK, Apr. 21, 2010, http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=224500173&subSection=News ("Many observers […] have come to the conclusion that the government's cybersecurity reporting requirements, as currently implemented, have created an environment in which expensive annual compliance reports that cut into real cybersecurity have become the norm.").

[1076] OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-10-15, FY 2010 REPORTING INSTRUCTIONS FOR THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT AND AGENCY PRIVACY MANAGEMENT (2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

statement about what Federal entities should concentrate resources on" and requires a "three-tiered approach" that entails (1) data feeds directly from security management tools (termed "continuous monitoring" by the OMB); (2) government-wide benchmarking on security posture similar to the previously required reports; and (3) agency-specific interviews.[1077] The memorandum requires that all reporting be performed by using DHS's online reporting platform CyberScope[1078] but neither states which information would be subject to "continuous monitoring" nor discloses the actual metrics that will be used.

The following preliminary observations can be made nonetheless: First, the term "continuous monitoring" is misleading as OMB Memorandum M-10-15 indeed only requires monthly data feeds.[1079] Second, "continuous monitoring" seems to be limited to the monitoring of assets and security controls,[1080] disregarding other risk components,[1081] in particular threats. Whether the new reporting requirements will indeed change the way FISMA affects information security at federal agencies remains to be seen.

[1077] *See id.* at 1.

[1078] *See* https://max.omb.gov/community/x/EgQrFQ (last accessed Feb. 10, 2011). *Cf. also* David Perera, *OMB gives DHS new powers under revised FISMA guidance*, FIERCEGOVERNMENTIT, Apr. 21, 2010, http://www.fiercegovernmentit.com/story/omb-gives-dhs-new-powers-under-revised-fisma-guidance/2010-04-21.

[1079] OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-10-15, FY 2010 REPORTING INSTRUCTIONS FOR THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT AND AGENCY PRIVACY MANAGEMENT 2 (2010).

[1080] *See id.* at 2 (stating that the new data feeds will include summary information in the following areas: inventory; systems and services; hardware; software; external connections; security training; and identity management and access). *See also id.* at 11 (referring to the "[c]ontinuous monitoring of security controls"). *Cf.* Richard Bejtlich, *Thoughts on New OMB FISMA Memo*, TAOSECURITY, Apr. 24, 2010, http://taosecurity.blogspot.com/2010/04/thoughts-on-new-omb-fisma-memo.html (emphasizing the lack of threat monitoring).

[1081] *Cf.* chapter 3.1 (defining the following risk components: asset, safeguard, vulnerability, threat, and threat agent).

In addition to FISMA's reporting requirements, the way it allocates and enforces responsibility for FISMA compliance has also been criticized in the past: FISMA allocates an agency's internal responsibility with the head of the agency.[1082] However, he or she has to delegate the authority to ensure FISMA compliance to the agency's Chief Information Officer (CIO)[1083] who, in turn, has to designate a senior agency information security officer to carry out the CIO's responsibilities under FISMA,[1084] ultimately making it rather difficult to decide who is to blame in case of non-compliance.[1085] Furthermore, FISMA does not foresee the enforcement of individual accountability. It rather allows the OMB to take action against an agency as a whole by reducing agency budgets or appropriations for information resources,[1086] otherwise restricting the availability of amounts for information resources,[1087] or designating an executive agent to outsource information resources management or IT acquisition.[1088] The first two options may indeed be very counterproductive and are therefore unlikely to be imposed[1089] while the third might indeed not be much of a "punishment" for overworked and underfunded CIOs.[1090]

[1082] *See* 44 U.S.C. § 3544(a).

[1083] *See* 44 U.S.C. § 3544(a)(3).

[1084] *See* 44 U.S.C. § 3544(a)(3)(A).

[1085] *See* Robert Silvers, *Rethinking FISMA and Federal Information Security Policy,* 81 N.Y.U. L. REV. 1844, 1863 (2006) (criticizing these roles by stating that "[t]his kind of overlapping and duplicative responsibility breeds the administrative inertia and complacency for which bureaucracies are (in)famous" (citing PAUL C. LIGHT, THICKENING GOVERNMENT: FEDERAL HIERARCHY AND THE DIFFUSION OF ACCOUNTABILITY 64 (1995))).

[1086] *See* 44 U.S.C. § 3543(a)(4) in conjunction with 40 U.S.C. § 11303(b)(5)(B)(i) and (ii).

[1087] *See id.* § 11303(b)(5)(B)(iii).

[1088] *See id.* § 11303(b)(5)(B)(iv).

[1089] *See* Robert Silvers, *Rethinking FISMA and Federal Information Security Policy,* 81 N.Y.U. L. REV. 1844, 1863 (2006). Indeed, no sanctions for non-compliance with FISMA have been reported so far.

[1090] *See id*.

In summary, FISMA establishes reasonable security requirements, including mandatory security controls for federal information systems. Its compliance monitoring and enforcement mechanisms, however, show significant deficiencies.

4.4.2. Internal Security Regulations of the European Commission and the Council of the EU

Contrary to the U.S., the EU has not adopted any legislative measures that would mandate security controls for any of its institutions. However, it has to be pointed out that such a legislative measure is significantly less important in the EU: First, the European Commission is in size only about 2.7% of the executive branch of the U.S. federal government.[1091] Second, the European Commission generally does not directly implement EU law.[1092] Accordingly, the EU institutions maintain significantly fewer information assets than the executive branch of the U.S. federal government.

It is therefore not surprising that the European Commission and the Council have addressed information security issues in their internal Rules of Procedure from a much narrower perspective than FISMA: Based on article 24 of its Rules of Procedure,[1093] the Council has

[1091] As of Nov. 2008, the executive branch of the U.S. federal government, excluding the U.S. postal service and defense departments and agencies had 1,194,000 civilian employees. *See* http://www.bls.gov/oco/cg/cgs041.htm (last accessed Feb. 10, 2011). For the fiscal year of 2010, the European Commission, including EU agencies, has allocated a budged for 31,596 officials and temporary agents. *See* http://eur-lex.europa.eu/budget/data/D2010_ VOL1/EN/nmc-grseqAP2000182/index.html (last accessed Feb. 10, 2011).

[1092] *Cf.* JÜRGEN SCHWARZE, EUROPEAN ADMINISTRATIVE LAW, at clxix (2006) (stating that, as a general rule, EU law is not directly implemented by EU authorities but rather indirectly implemented by the administrative authorities of the Member States); Stefan Storr, *Grundsätze des Verwaltungsverfahrens aus gemeinschaftsrechtlicher Sicht* [*Principles of the Administrative Procedure from a Community Law Perspective*], *in* ABGABEVERFAHRENSRECHT UND GEMEINSCHAFTSRECHT [PUBLIC CHARGES PROCEDURAL LAW AND COMMUNITY LAW] 13, 15 (Michael Holoubek & Michael Lang eds., 2006). Note that EU competition law is the most notable exception to this general rule.

[1093] Council Decision 2009/937 of 1 December 2009, art. 24, 2009 O.J. (L 325) 35, 49 (EU) (“The rules on security shall be adopted by the Council acting by a qualified majority.”).

adopted its Rules on Security[1094] which cover physical, administrative, and technical aspects of information security but only apply to "classified information."[1095] Similarly, the Commission's Rules on Security,[1096] adopted as an annex to its Rules of Procedure,[1097] also only cover "classified information."[1098]

4.4.3. Comparative Assessment

The U.S.'s and the EU's regulatory regimes discussed *supra* in chapters 4.4.1 and 4.4.2 differ greatly with regard to their scope of application. While FISMA applies to all information and information systems within federal agencies, the Security Rules of the Commission and the Council only apply to classified information, thereby rendering the Security Rules virtually irrelevant outside relatively small parts of these institutions.

FISMA, on the other hand, had a significant effect on the entire executive branch of the U.S. federal government as well as on government contractors, but this effect was not necessarily positive: by establishing metrics that measured the extent and completeness of documentation rather than the effectiveness of actually implemented safeguards,[1099] FISMA caused federal

[1094] Council Decision 2001/264 of 19 March 2001, 2001 O.J. (L 101) 1.

[1095] *Id.* art. 2(1) (stating that the Council's security regulations are only to be respected "when handling EU classified information").

[1096] Initially introduced by Commission Decision 2001/844, 2001 O.J. (L 317) 1.

[1097] Commission Rules of Procedure, 2000 O.J. (L 308) 26 as amended. A consolidated version of the Commission's Rules of Procedure, including its Rules on Security is available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2000Q3614:20100306:EN:PDF (last accessed Feb. 10, 2011).

[1098] Commission Decision 2001/844, art. 2(1), 2001 O.J. (L 317) 1, 2 (stating that the Commission's rules on security are only to be respected "when handling EU classified information").

[1099] *Cf.* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 54 (2d ed. 2010) (noting that the U.S. Department of Veterans Affairs' "previous approach to measuring [...] focused on counting the number of people who completed certain security training courses and the number of desktops that had certain systems installed. In other words, the VA wasn't measuring results at all. All previous measurement efforts focused on what was considered easy to measure.").

agencies to spend very significant resources on paperwork instead of actually improving security. The lesson that should, and indeed seems to have been learned[1100] from the past experience with FISMA is that better metrics are needed if metrics are to be used in the enforcement process.[1101] In this regard, policy makers face the same challenges as any CEO of a large corporation who wishes to introduce corporation-wide security metrics.[1102]

Lastly, it should be noted that any policy that exclusively focuses on government authorities is unlikely to effectively address any of the fundamental challenges of information security.[1103] Such a policy may nonetheless at least improve the level of information security at government authorities which, depending on the number and size of covered government authorities, may in itself be a significant step.

4.5. Mandatory Security Controls for Software Manufacturers

As discussed *supra* in chapter 2.3.3, software manufactures are essential players in the information security landscape because software-based vulnerabilities have a very significant effect on information security in general. However, regulation that would require software manufacturers to implement security controls in an effort to increase the level of information security provided by their products is largely absent. The only two areas in which notable

[1100] *See supra* chapter 4.4.1 (discussing OMB's attempt to establish new metrics for the fiscal year of 2010).

[1101] Hubbard refers to an objection to measurement that is based on the assertion that it influences third parties in unintended ways as a variation of the "economic objection." This is to be seen as distinct from the three misconceptions of measurement briefly discussed *supra* in chapter 2.4.3. *See* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 36 (2d ed. 2010).

[1102] *Cf.* W. KRAG BROTBY, INFORMATION SECURITY MANAGEMENT METRICS: A DEFINITIVE GUIDE TO EFFECTIVE SECURITY MONITORING AND MEASUREMENT 5 (2009) (noting that "most senior management has yet to understand that like every other aspect of business, optimal and cost-effective security, or IT operations generally, cannot be attained without appropriate feedback mechanisms to gauge direction and performance").

[1103] *See supra* chapter 2.4.

regulatory action was taken are medical devices (see *infra* chapters 4.5.1 and 4.5.2) and electronic signature products (see *infra* chapter 4.5.3).

Medical devices are often only marginally concerned with information security and focus much more on personal safety. Regulatory regimes that address such devices are discussed here nonetheless for two reasons: First, personal safety often depends on the security (in particular the availability and integrity) of the information stored, processed, or transmitted by these devices. Second, the regulatory domain of medical devices is rather heterogeneous when compared to electronic signature products, making it particularly relevant in the context of more general considerations of software security.

4.5.1. Federal Food, Drug, and Cosmetic Act

Section 520(f)(1)[1104] of the Federal Food, Drug, and Cosmetic Act[1105] (hereinafter *FFDCA*) provides the Food and Drug Administration (FDA) with the authority to prescribe regulations requiring that the methods used in the manufacture, pre-production design validation,[1106] packing, storage, and installation of a medical "device"[1107] conform to current good manufacturing practice, as prescribed in such regulations.[1108]

[1104] 21 U.S.C. § 360j(f)(1) (2010).

[1105] Pub. L. No. 75-717, 52 Stat. 1040 (1938) (codified as amended at 21 U.S.C. § 301 et seq.).

[1106] FFDCA § 520(f)(1), 21 U.S.C. § 360j(f)(1) provides that this includes "a process to assess the performance of a device but not […] an evaluation of the safety or effectiveness of a device." "[P]re-production design validation" was inserted into § 520(f)(1) by Safe Medical Devices Act of 1990, Pub. L. 101-629, § 18(e), 104 Stat. 4511, 4529 (1990).

[1107] *See* FFDCA § 201(h), 21 U.S.C. § 321(h) (defining "device" as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is—(1) recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them, (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or (3) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes

In particular on this legal basis,[1109] the FDA has adopted the Quality System Regulation[1110] which applies to all manufacturers of finished[1111] medical devices intended for human use.[1112] Significantly, the Quality System Regulation covers software that is used as a component in a medical device[1113] or that is itself a medical device.[1114]

The Quality System Regulation requires manufacturers to establish (i.e. define, document, and implement)[1115] and maintain a "quality system" that is appropriate for the specific medical device(s) designed or manufactured.[1116] Such a quality system has to comprise

through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes").

[1108] *See* FFDCA § 520(f)(1), 21 U.S.C. § 360j(f)(1).

[1109] *Cf.* 21 C.F.R. § 820.1(c) (providing a list of all statutory provisions that serve as a legal basis for the Quality System Regulation). One of the provisions that serve as a legal basis is FFDCA § 510, 21 U.S.C. § 360 which requires a premarket notification to the FDA. For more information about premarket submissions for software contained in medical devices see FDA, GUIDANCE FOR THE CONTENT OF PREMARKET SUBMISSIONS FOR SOFTWARE CONTAINED IN MEDICAL DEVICES (2005), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089593.pdf.

[1110] 61 Fed. Reg. 52,602 (Oct. 7, 1996) (codified as amended at 21 C.F.R. pt. 820).

[1111] *See* 21 C.F.R. § 820.3(l) (defining "finished device" as "any device or accessory to any device that is suitable for use or capable of functioning, whether or not it is packaged, labeled, or sterilized").

[1112] *See* 21 C.F.R. § 820.1(a).

[1113] *See* 21 C.F.R. § 820.3(c) (defining "component" as "any raw material, substance, piece, part, *software*, firmware, labeling, or assembly which is intended to be included as part of the finished, packaged, and labeled device" (emphasis added)).

[1114] *Cf.* 21 C.F.R. § 820.3(m) (defining "lot or batch" as "one or more components or finished devices that consist of a single type, model, class, size, composition, or *software version* that are manufactured under essentially the same conditions and that are intended to have uniform characteristics and quality within specified limits" (emphasis added)). *Cf. also* 61 Fed. Reg. 52,602, 52,602 (Oct. 7, 1996) (emphasizing the significance of design-related errors regarding software used to operate medical devices). Note that the Quality System Regulation also covers and imposes essentially the same requirements for a third category of software: software that is used to automate any part of the device production process or any part of the quality system. 21 C.F.R. § 820.70(i). However, since this chapter focuses on *software* manufacturers—and not on manufacturers of other products that merely use software in the manufacturing process—this third category of covered software will not be discussed here. For a general discussion of the regulatory background of medical device software see E. Stewart Crumpler & Harvey Rudolph, *FDA Software Policy and Regulation of Medical Device Software*, 52 FOOD & DRUG L.J. 511 (1997).

[1115] *See* 21 C.F.R. § 820.3(k).

[1116] *See* 21 C.F.R. § 820.5.

"organizational structure, responsibilities, procedures, processes, and resources for implementing quality management."[1117] In particular, it is the management's responsibility to establish and maintain (1) a quality policy, (2) an adequate organizational structure, (3) management review procedures, (4) a quality plan, and (5) quality system procedures.[1118] Manufacturers also have to perform quality audits to determine the degree of compliance and effectiveness of the quality system[1119] and have to have sufficient personnel with the necessary education, background, training, and experience to assure that all activities are correctly performed.[1120]

Furthermore, the Quality System Regulation requires manufacturers to establish and maintain procedures (1) to control all documents required by the regulation;[1121] (2) to ensure that all purchased or otherwise received product and services conform to specified requirements;[1122] (3) to identify a product during all stages of its lifecycle;[1123] (4) to control manufacturing

[1117] *See* 21 C.F.R. § 820.3(m) (defining the term "quality system"). *See also* 21 C.F.R. § 820.20 (establishing management responsibility for: (1) implementation of a quality policy, (2) organization, (3) management review, (4) quality planning, (5) quality system procedures), § 820.22 (requiring quality audits to determine compliance and effectiveness of the quality system), and § 820.25 (mandating that each manufacturer has sufficient personnel with the necessary education, background, training, and experience to assure that all activities are correctly performed).

[1118] *See* 21 C.F.R. § 820.20(a)-(e).

[1119] *See* 21 C.F.R. § 820.22.

[1120] *See* 21 C.F.R. § 820.25.

[1121] *See* 21 C.F.R. § 820.40.

[1122] *See* 21 C.F.R. § 820.50.

[1123] *See* 21 C.F.R. § 820.60.

processes;[1124] and (5) to control the design of the device in order to ensure that specified design requirements are met.[1125]

The last-mentioned "design controls" are of particular relevance for software: In contrast to hardware, the quality of software primarily depends on design and development with only a minimum concern for the manufacturing process (which typically only consists of creating another copy of the software).[1126] The required design controls are: (1) design and development planning;[1127] (2) procedures to ensure that the design requirements ("design input") are appropriate and address the intended use of the device;[1128] (3) procedures for defining and documenting design output in terms that allow an adequate evaluation of conformance to design requirements;[1129] (4) design review procedures;[1130] (5) procedures to confirm that the design output meets the design requirements ("design verification");[1131] (6) procedures to ensure that devices conform to defined user needs and intended uses ("design

[1124] *See* 21 C.F.R. §§ 820.70, .72, .75.

[1125] *See* 21 C.F.R. § 820.30. Note that there are some devices that are not subject to the device control requirements; however, all devices "automated with computer software" are. *See* 21 C.F.R. § 820.30(a)(2).

[1126] *See* FDA, GENERAL PRINCIPLES OF SOFTWARE VALIDATION; FINAL GUIDANCE FOR INDUSTRY AND FDA STAFF 8 (2002), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf (discussing the reasons why software is different from hardware as regards quality management). *Cf.* 61 Fed. Reg. 52,602, 52,602 (Oct. 7, 1996) (referring to FDA, EVALUATION OF SOFTWARE RELATED RECALLS FOR FISCAL YEARS 1983-91 (1992), which found that over 90% of all software-related device failures were due to design-related errors).

[1127] *See* 21 C.F.R. § 820.30(b).

[1128] *See* 21 C.F.R. § 820.30(c). *Cf.* 21 C.F.R. § 820.3(f) (defining "design input" as "the physical and performance requirements of a device that are used as a basis for device design").

[1129] *See* 21 C.F.R. § 820.30(d). *Cf.* 21 C.F.R. § 820.3(g) (defining "design output" as "the results of a design effort at each design phase and at the end of the total design effort […]").

[1130] *See* 21 C.F.R. § 820.30(e). *Cf.* 21 C.F.R. § 820.3(h) (defining "design review" as "a documented, comprehensive, systematic examination of a design to evaluate the adequacy of the design requirements, to evaluate the capability of the design to meet these requirements, and to identify problems").

[1131] *See* 21 C.F.R. § 820.30(f). *Cf.* 21 C.F.R. § 820.3(aa) (defining "verification" as "confirmation by examination and provision of objective evidence that specified requirements have been fulfilled").

validation");[1132] (5) procedures to ensure that the design is correctly translated into production specifications ("design transfer");[1133] and (6) procedures for the identification, documentation, validation or, where appropriate, verification, review, and approval of design changes.[1134]

As regards software, design validation has been of particular concern for manufacturers, prompting the FDA to publish General Principles of Software Validation[1135] which the FDA considers the "least burdensome" (but by no means the only) way to comply with the design validation requirements.[1136] In it, the FDA explains that software validation is part of the design validation for a finished device and defines it as "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled."[1137] The General Principles of Software Validation further provide that

[1132] *See* 21 C.F.R. § 820.30(g). *Cf.* 21 C.F.R. § 820.3(z)(3) (defining "design validation" as "establishing by objective evidence that device specifications conform with user needs and intended use(s)").

[1133] *See* 21 C.F.R. § 820.30(h).

[1134] *See* 21 C.F.R. § 820.30(i).

[1135] *See* FDA, GENERAL PRINCIPLES OF SOFTWARE VALIDATION; FINAL GUIDANCE FOR INDUSTRY AND FDA STAFF (2002), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf.

[1136] *See id*. at 2. *Cf. also* United States v. Utah Med. Products, Inc., 404 F. Supp. 2d 1315, 1324 (D. Utah 2005) (holding with regard to similar guidance documents—ASSOC. FOR THE ADVANCEMENT OF MEDICAL INSTRUMENTATION, THE QUALITY SYSTEM COMPENDIUM (1998) and THE GLOBAL HARMONIZATION TASK FORCE, QUALITY MANAGEMENT SYSTEMS – PROCESS VALIDATION GUIDANCE (2004), *available at* http://www.ghtf.org/documents/sg3/sg3_fd_n99-10_edition2.pdf—that they "may be of some value as evidence of some standards suitable for some manufacturers, but in no sense are specifically embraced by the regulations, nor have changes been made in the regulations to incorporate them").

[1137] FDA, GENERAL PRINCIPLES OF SOFTWARE VALIDATION; FINAL GUIDANCE FOR INDUSTRY AND FDA STAFF 6 (2002). Note that software *validation* is distinct from software *verification*. Software verification helps to ensure that "software was build right" while software validation helps to ensure that the "right software was built." LINDA WESTFALL, THE CERTIFIED SOFTWARE QUALITY ENGINEER HANDBOOK, at xxiv, 386 et seq. (2010).

the "level of confidence" needed to allow a manufacturer to conclude that software is validated depends on the risk associated with the software and its intended uses.[1138]

To a significant extent, software validation is supported by the other design controls referred to above.[1139] Additionally, manufactures should consider (1) source code reviews;[1140] (2) software testing;[1141] and (3) the validation of software changes.[1142] The General Principles of Software Validation discuss in particular and extensively software testing and correctly point out that "[e]xcept for the simplest of programs, software cannot be exhaustively tested."[1143] Software testing is therefore considered only one of many components of successful software validation.[1144]

To establish a violation of the Quality System Regulation, the FDA must prove by a preponderance of evidence that "the quality assurance program is not adequate to assure and verify confidence in the quality of the process used […] to manufacture the [device] or that a specific minimum requirement set forth in the [Quality System Regulation] is inadequate or missing from the quality assurance program."[1145] Enforcement options against manufacturers

[1138] FDA, GENERAL PRINCIPLES OF SOFTWARE VALIDATION; FINAL GUIDANCE FOR INDUSTRY AND FDA STAFF 7, 31 (2002).

[1139] *Cf. id.* at 15 (discussing quality planning; *see* 21 C.F.R. § 820.30(b)), 16 (discussing requirements development; *see* 21 C.F.R. § 820.30(c)), and 17 (discussing the software design process and design review; *see* 21 C.F.R. § 820.30(d) and (e)).

[1140] *See id.* at 20.

[1141] *See id.* at 21-28.

[1142] *See id.* at 28.

[1143] *See id.* at 22.

[1144] *Cf. id.* at 8 (noting that, in addition to software testing, "other […] techniques and a structured and documented development process should be combined to ensure a comprehensive validation approach").

[1145] United States v. Laerdal Mfg. Corp., 853 F. Supp. 1219, 1227 (D. Or. 1994), *aff'd*, 73 F.3d 852 (9th Cir. 1995).

which violate the Quality System Regulation include injunctions,[1146] civil penalties,[1147] and the inclusion of the manufacturer on an FDA-internal "reference list" which bars a manufacturer both from FDA approvals and from government purchasing contracts.[1148]

4.5.2. EU Medical Devices Directive

Council Directive 93/42[1149] (hereinafter *Medical Devices Directive*) covers medical devices intended by the manufacturer to be used for human beings, including devices which incorporate software or which are medical software in themselves.[1150]

Under the Directive, medical devices may only be placed on the market and/or put into service if they comply with the "essential requirements" laid down in annex I of the Directive.[1151] Manufacturers generally have to (1) eliminate or reduce risks as far as possible, (2) take adequate protection measures (e.g. alarms) in relation to risks that cannot be eliminated, and (3) inform users of the residual risks.[1152] Specifically regarding devices which

[1146] *See* 21 U.S.C. § 332 in conjunction with § 331(q)(1)(A). *Cf., e.g., Radiation Treatment Software Maker Signs Consent Decree*, FDA ENFORCEMENT MANUAL NEWSL. (Thompson Publishing Group, Tampa, Fla.), Oct. 2003.

[1147] *See* 21 U.S.C. § 333 in conjunction with § 331(q)(1)(A). *Cf.* Nancy W. Mathewson, *Prohibited Acts and Enforcement Tools*, 65 FOOD & DRUG L.J. 545, 548 (2010).

[1148] *Cf.* Donald E. Segal, *New Enforcement Initiatives—An Industry View*, 47 FOOD DRUG COSM. L.J. 421, 428 (1992); JAMES T. O'REILLY, 1 FOOD AND DRUG ADMINISTRATION § 18:126 (3rd ed. 2010).

[1149] 1993 O.J. (L 169) 1 (EEC) as amended.

[1150] Medical Devices Directive art. 1(2)(a). Parliament and Council Directive 2007/47, 2007 O.J. (L 247) 21 (EC) clarified that "software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, is a medical device." *Id.* recital 6. Note that the Medical Devices Directive does not cover active implantable medical devices (e.g. a pacemaker) and in vitro diagnostic medical devices which are covered by Council Directive 90/385, 1990 O.J. (L 189) 17 (EEC) (as amended) and Parliament and Council Directive 98/79, 1998 O.J. (L 331) 1 (EC) (as amended) respectively. *Cf. generally* ARND PANNENBECKER, MÜNCHENER ANWALTSHANDBUCH MEDIZINRECHT [MUNICH ATTORNEY HANDBOOK MEDICAL LAW] § 9.II.1.a (Michael Terbille ed., 2009).

[1151] *See* Medical Devices Directive art. 2 and 3.

[1152] Medical Devices Directive annex I.2.

incorporate software or which are medical software in themselves, annex I requires that the software "be validated according to the state of the art taking into account the principles of development lifecycle, risk management, validation and verification."[1153]

According to Medical Devices Directive article 5, compliance with the essential requirements is to be presumed if the device in question is in conformity with national standards adopted pursuant to the harmonized standards the references of which have been published by the Commission in the Official Journal.[1154] As of December 2010, the only such standard which specifically addresses software is IEC 62304:2006, entitled "Medical device software – Software life cycle processes."[1155] This standard, without prescribing a specific life cycle model, provides a framework of processes with associated activities and tasks covering software development and verification,[1156] software maintenance,[1157] software risk

[1153] Medical Devices Directive annex I.12.1a. This software-specific requirement was introduced by Parliament and Council Directive 2007/47, annex II.1.g, 2007 O.J. (L 247) 21, 44 (EC). It has to be enforced by Member States since Mar. 21, 2010. *Id.* art. 4(1). Note that no further guidance is provided for interpreting this requirement. Council Directive 2007/47 recital 20 only notes that "[t]aking account of the growing importance of software in the field of medical devices […] validation of software in accordance with the state of the art should be an essential requirement."

[1154] In this regard, the Commission is assisted by the Committee on Standards and Technical Regulations which consists of representatives appointed by the Member States and is chaired by a representative of the Commission. Medical Devices Directive art. 6 in conjunction with Parliament and Council Directive 98/34, art. 5, 1998 (L 204) 37, 41 (EC). Note that Medical Devices Directive recital 12 only recognizes the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (Cenelec) as competent bodies for the adoption of harmonized medical device standards.

[1155] *See* Commission communication in the framework of the implementation of the Council Directive 93/42/EEC concerning medical devices, 2008 O.J. (C 304) 8, 16 and Commission communication in the framework of the implementation of the Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, 2010 O.J. (C 183) 15, 43 (both referring to INT'L ELECTROTECHNICAL COMM'N [IEC], MEDICAL DEVICE SOFTWARE – SOFTWARE LIFE CYCLE PROCESSES, IEC 62304:2006 (2006) which has been adopted by Cenelec).

[1156] IEC, MEDICAL DEVICE SOFTWARE – SOFTWARE LIFE CYCLE PROCESSES, IEC 62304:2006 § 5 (2006).

[1157] *Id.* § 6.

management,[1158] software configuration management,[1159] and software problem resolution.[1160] Software validation, however, is explicitly excluded from the scope of IEC 62304:2006.[1161]

For a medical device to be placed on the market, it also has to bear the CE marking.[1162] A manufacturer may only affix the CE marking on a medical device if the conformity with the essential requirements has been assessed pursuant to article 11 of the Medical Devices Directive.[1163] Depending on the class the medical device falls into,[1164] different kinds of conformity assessment are required: Class I devices carry the lowest level of risk and generally only require a self-assessment;[1165] Class IIa devices require that certain parts of the assessment be performed by a "notified body";[1166] and Class IIb and III devices require an

[1158] *Id.* § 7.

[1159] *Id.* § 8.

[1160] *Id.* § 9.

[1161] *Id.* § 1.2 (noting that "[t]his standard does not cover validation […] of the MEDICAL DEVICE, even when the MEDICAL DEVICE consists entirely of software").

[1162] Medical Devices Directive art. 17. Pursuant to art. 4, Member States may "not create any obstacle to the placing on the market or the putting into service within their territory of devices bearing the CE marking." Note that exceptions exist for devices intended for clinical investigation and for custom-made devices. Medical Devices Directive art. 4(2). *Cf. also* Case C-288/08, Kemikalieinspektionen v. Nordiska Dental AB, 2009 E.C.R. I-11031, § 33 (holding that Medical Devices Directive art. 4(1) must be interpreted as precluding legislation of a Member State under which the commercial exportation of medical devices bearing the 'CE' marking is prohibited on grounds relating to protection of the environment and of health).

[1163] *Cf. generally* Sharon Frank, *An Assessment of the Regulations on Medical Devices in the European Union*, 56 FOOD & DRUG L.J. 99, 111 (2001).

[1164] *See* Medical Devices Directive art. 9 (referring to the classification criteria provided in annex IX). Software which drives a device or influences the use of a device, automatically falls in the same class as the device itself. Medical Devices Directive annex IX.2.3. For further discussion of the classification system and the difficulty of applying it novel devices the risk of which is still very uncertain see Giorgia Guerra, *A Model for Regulation of Medical Nanobiotechnology: The European Status Quo*, 3 NANOTECHNOLOGY L. & BUS. 84, 89 (2006). *Cf. also* Linda R. Horton, *Medical Device Regulation in the European Union*, 50 FOOD & DRUG L.J. 461, 469 (1995).

[1165] Medical Devices Directive art. 11(5) in conjunction with annex VII. In the case of devices with a measuring function, a notified body has to examine the production process with regard to the measuring function. Medical Devices Directive annex VII.5.

[1166] *See* Medical Devices Directive art. 11(2) in conjunction with annex VII, coupled with either annex IV, V, or VI. Notified bodies are designated by a Member State under the conditions set out in annex XI; they are typically private sector entities and remain answerable to the competent national authorities. *See* Medical Devices assessment by a notified body with regard to the design and manufacture of the devices.[1167] Manufacturers of devices that fall within Classes IIa, IIb, or III may choose from different conformity assessment approaches, some of which require an assessment of the manufacturer's quality system.[1168] In that case, conformity with EN ISO 13485:2003/AC:2009,[1169] which is based on ISO 9001,[1170] creates a presumption of compliance.[1171]

If the CE marking has been affixed unduly or is missing, the manufacturer is obliged to end the infringement under conditions imposed by the Member State.[1172] If a medical device, when correctly installed, maintained, and used for its intended purpose, may compromise the health and/or safety of patients, users, or other persons, Member States have to take measures to prohibit or restrict further distribution and use.[1173] If the non-complying device bears the

Directive art. 16. *Cf.* EUROPEAN COMM'N, GUIDE TO THE IMPLEMENTATION OF DIRECTIVES BASED ON THE NEW APPROACH AND THE GLOBAL APPROACH 36 (2000), *available at* http://ec.europa.eu/enterprise/policies/single-market-goods/files/blue-guide/guidepublic_en.pdf; John Chai, *Regulation of Medical Devices in the European Union*, 21 J. LEGAL MED. 537, 545 (2000).

[1167] With regard to Class IIb see Medical Devices Directive art. 11(3) in conjunction with (1) annex II (excluding annex II.4) or (2) annex III, coupled with either annex IV, V, or VI. Regarding Class III see Medical Devices Directive art. 11(1) in conjunction with (1) annex II or (2) annex III, coupled with either annex IV or V.

[1168] Medical Devices Directive annex II ("full quality assurance"), annex V ("production quality assurance"), and annex VI ("product quality assurance") require that the quality system be audited and periodically inspected by a notified body.

[1169] ISO, MEDICAL DEVICES – QUALITY MANAGEMENT SYSTEMS – REQUIREMENTS FOR REGULATORY PURPOSES, ISO 13485:2003/Cor 1:2009 (2009) (adopted by Cenelec as EN ISO 13485:2003/AC:2009).

[1170] *See id.* § 0.3.1. *Cf.* ISO, QUALITY MANAGEMENT SYSTEMS – REQUIREMENTS, ISO 9001:2008 (2008).

[1171] *Commission communication in the framework of the implementation of the Council Directive 93/42/EEC of 14 June 1993 concerning medical devices*, 2010 O.J. (C 183) 15, 25.

[1172] *See* Medical Devices Directive art. 18.

[1173] *See* Medical Devices Directive art. 8(1). Note that Member States have to immediately inform the Commission of any such measures, allowing the Commission to determine, after a consultation with the parties concerned, whether the measures are justified. Medical Devices Directive art. 8(2).

CE marking, the competent Member State also has to take "appropriate action" against whoever has affixed the marking (e.g. the manufacturer).[1174]

4.5.3. EU eSignature Directive

Parliament and Council Directive 1999/93[1175] (hereinafter *eSignature Directive*) provides that electronic signatures only have to be recognized as equivalent to handwritten signatures if, *inter alia*,[1176] they are created by a "secure-signature-creation device."[1177] Such a device can consist in software and/or hardware[1178] and is considered "secure" if it meets the requirements laid down in annex III of the Directive.[1179]

Annex III provides that a secure signature-creation device must ensure that (1) the private keys (referred to as "signature-creation-data") used for signature generation can practically occur only once;[1180] (2) the confidentiality of private keys is reasonably assured;[1181] (3) private keys cannot, with reasonable assurance, be derived;[1182] (4) the signature is protected

[1174] *See* Medical Devices Directive art. 8(2). Note that no guidance is provided as to what is "appropriate."

[1175] 2000 O.J. (L 13) 12 (EC) as amended by Parliament and Council Regulation No. 1137/2008, 2008 O.J. (L 311) 1 (EC). For a brief introduction see *supra* chapter 4.3.3.

[1176] *Cf. supra* chapter 4.3.3 (discussing the other requirements).

[1177] *See* eSignature Directive art. 5(1).

[1178] *See* eSignature Directive art. 2(5) (defining "signature-creation device" as "configured software or hardware used to implement the signature-creation data" (i.e. the cryptographic private key)).

[1179] *See* eSignature Directive art. 2(6).

[1180] *See* eSignature Directive annex III.1.a. Asymmetric cryptographic keys typically have a length of at least 2048 bits. NIELS FERGUSON ET AL., CRYPTOGRAPHY ENGINEERING: DESIGN PRINCIPLES AND PRACTICAL APPLICATIONS 203 (2010). This means that there are 2^{2048} or about 10^{616} different possible keys, making it very unlikely that two identical keys will ever be generated.

[1181] *See* eSignature Directive annex III.1.a. Asymmetric cryptography is built on the assumption that the private key remains confidential to the signatory. If any third party obtains the private key, neither authenticity, non-repudiation, nor integrity of signed information can be established any longer. *Cf.* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 182 (2d ed. 1996) (discussing the devastating effects of a compromised private key).

[1182] *See* eSignature Directive annex III.1.b. For a general discussion of various attacks that can potentially be used to derive the private key from the public key, from a known encrypted text, or from external indicators such against forgery using currently available technology;[1183] (5) the private keys can be reliably protected by the legitimate signatory against the use of others;[1184] (6) data to be signed is not altered;[1185] (7) data to be signed is not prevented from being presented to the signatory prior to the signature process.[1186] With regard to the last requirement, it should be emphasized that secure signature-creation devices do not have to implement the critical functionality of data presentation themselves.

The conformity of secure signature-creation-devices with annex III has to be determined by appropriate public or private bodies designated by the Member States,[1187] whereby a determination of conformity made by one such body has to be recognized by all Member States.[1188] A presumption of compliance is created if a secure signature-creation-device complies with a generally recognized standard a reference to which has been published by the Commission in the Official Journal. The only such standard adopted by the Commission is CWA 14169:2002.[1189]

as power consumption or electromagnetic radiation see BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 5 et seq. (2d ed. 1996); SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 753 et seq. (4th ed. 2008).

[1183] *See* eSignature Directive annex III.1.b.

[1184] *See* eSignature Directive annex III.1.c. This requirement acknowledges that having access to the process that generates a signature is sufficient to forge signatures—even if the private key is not disclosed.

[1185] *See* eSignature Directive annex III.2.

[1186] *See id.*

[1187] *See* eSignature Directive art. 3(4). Beyond explicitly stating that conformity assessments have to be recognized by all member states, the Directive is indeed not entirely clear as to whether a conformity assessment is legally required. *See* SEALED ET AL., STUDY ON CROSS-BORDER INTEROPERABILITY OF ESIGNATURES (CROBIES), FRAMEWORK FOR SECURE SIGNATURE CREATION DEVICES CROSS-BORDER RECOGNITION 14 (2010), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd4.pdf.

[1188] *See id.*

[1189] CEN, SECURE SIGNATURE-CREATION DEVICES "EAL 4+," CEN WORKSHOP AGREEMENT CWA 14169:2002 (2002), *available at* http://www.a-sit.at/pdfs/cwa14169.pdf. It was adopted by the Commission in 2003. Commission Decision 2003/511, 2003 O.J. (L 175) 45, 46 (EC).

Similar to the standards adopted with regard to "trustworthy systems and products" for certification-service-providers,[1190] this standard exhibits a number of significant deficiencies: First, it is outdated. CWA 14169:2002 has long been superseded by CWA 14169:2004.[1191] However, the Commission has not yet published a reference to the updated standard. This means that the standard which creates a presumption of compliance is indeed not "state of the art." Even more significant from a practical perspective, CWA 14169:2002 has expired, making certifications pursuant to the Common Criteria[1192] impossible.[1193]

Second, CWA 14169:2002—as well as CWA 14169:2004—contains a normative reference to a certain "list of algorithms and parameters" which is indeed inexistent.[1194] This further adds to the unsuitability of CWA 14169:2002 for any certification purposes.

Third, annex III and therefore CWA 14169 is fundamentally flawed because its scope is too narrow to provide reasonable assurance that electronic signatures created with a secure signature-creation-device indeed establish authenticity, non-repudiation, and integrity: any system that provides these features, must not only provide a component that handles the

[1190] *See supra* chapter 4.3.3.

[1191] CEN, SECURE SIGNATURE-CREATION DEVICES "EAL 4+," CEN WORKSHOP AGREEMENT CWA 14169:2004 (2004), *available at* ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14169-00-2004-Mar.pdf.

[1192] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – EVALUATION CRITERIA FOR IT SECURITY – PART 1: INTRODUCTION AND GENERAL MODEL, ISO/IEC 15408-1:2009 (2009).

[1193] *See* SEALED ET AL., STUDY ON CROSS-BORDER INTEROPERABILITY OF ESIGNATURES (CROBIES), FRAMEWORK FOR SECURE SIGNATURE CREATION DEVICES CROSS-BORDER RECOGNITION 38 (2010), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd4.pdf.

[1194] All three Protection Profiles contained in CWA 14169:2002 refer to a "list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive." However, no such list exists. *Cf.* SEALED ET AL., STUDY ON CROSS-BORDER INTEROPERABILITY OF ESIGNATURES (CROBIES), FRAMEWORK FOR SECURE SIGNATURE CREATION DEVICES CROSS-BORDER RECOGNITION 49 (2010), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd4.pdf (concluding that this not only leads to a situation where each country may establish its own criteria but also creates a risk that art. 3(5) cannot be followed anymore, i.e. no presumption of compliance with annex III will be created).

private key (i.e. the secure signature-creation-devices),[1195] it must furthermore, provide components that handle the data to be signed, and provide a human interface device for display of the data to be signed and input of the signatory authentication data.[1196] In particular without a secure human interface device, the signatory will have no assurance that the displayed document is actually the one being signed. As *Ross Anderson* writes, "[t]he end result will be a 'secure' (in the sense of non-repudiable) signature on whatever the virus or Trojan [horse] in your PC sent to your [secure-signature-creation device]."[1197]

In summary, the eSignature Directive only focuses on one of multiple components needed to provide assurance for electronic signatures. Furthermore, the standard that has been adopted for this specific component—secure signature-creation-devices—is, for multiple reasons, inadequate to serve as a basis for product certifications.

4.5.4. Comparative Assessment

The different regulatory regimes requiring software manufacturers to implement security controls are first assessed with regard to the role of third parties (see *infra* chapter 4.5.4.1). The assessment will then turn to one of the most fundamental questions of regulating software quality: whether to focus on quality control or on quality assurance (see *infra* chapter 4.5.4.2).

[1195] *Cf.* eSignature Directive art. 2(5) (defining "signature-creation device" as "configured software or hardware *used to implement the signature-creation data*" (i.e. the private key; emphasis added)).

[1196] *See* SEALED ET AL., STUDY ON CROSS-BORDER INTEROPERABILITY OF ESIGNATURES (CROBIES), FRAMEWORK FOR SECURE SIGNATURE CREATION DEVICES CROSS-BORDER RECOGNITION 39, 50 (2010), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd4.pdf. *Cf. also* SEALED ET AL., STUDY ON THE STANDARDIZATION ASPECTS OF ESIGNATURE 32 (2007), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/standardisation/report_esign_standard.pdf (pointing out the lack of standardized cryptographic components for the creation *and the validation* of electronic signatures).

[1197] ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 878 (2d ed. 2008).

4.5.4.1. The Role of Third Parties

The Federal Food, Drug, and Cosmetic Act (FFDCA) implements a traditional regulatory approach by assigning primary responsibilities for adopting and enforcing regulatory standards to the FDA, a regulatory agency. While standards other than the FDA's General Principles of Software Validation can also be followed to achieve compliance with the Quality System Regulation's design control requirements, it remains the FDA's sole responsibility to assess whether the implementation of these alternative standards meets the regulatory requirements.

The Medical Devices Directive and the eSignature Directive, on the other hand, implement the "New Approach"[1198] and make third parties a cornerstone of their regulatory processes. Both directives provide that the compliance with regulatory requirements is primarily to be assessed by (typically private) bodies designated by the Member States.[1199] Furthermore, the directives rely on European standardization organizations to develop standards that, if subsequently adopted by the Commission, create a presumption of compliance for all products and processes that conform to it.

This approach seems to work for the Medical Devices Directive pursuant to which reasonable standards have been approved for software life cycle processes[1200] and quality systems.[1201] The eSignature Directive, on the other hand, demonstrates some of the risks associated with

[1198] The "New Approach" was launched by Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards, 1985 O.J. (C 136) 1. *See also supra* chapter 4.3.4.1 (providing a brief introduction into and further references for the "New Approach").

[1199] "Notified bodies" in the case of the Medical Devices Directive and "appropriate public or private bodies designated by Member States" in the case of the eSignature Directive. *See supra* chapters 4.5.2 and 4.5.3.

[1200] *See* IEC, MEDICAL DEVICE SOFTWARE – SOFTWARE LIFE CYCLE PROCESSES, IEC 62304:2006 (2006).

[1201] *See* ISO, MEDICAL DEVICES – QUALITY MANAGEMENT SYSTEMS – REQUIREMENTS FOR REGULATORY PURPOSES, ISO 13485:2003/Cor 1:2009 (2009) (adopted by Cenelec as EN ISO 13485:2003/AC:2009).

the "New Approach"[1202]: (1) the standardization organizations tasked with developing a standard for secure signature-creation-devices have created deficient standards that contain inexistent references;[1203] and (2) the standard a reference to which has been published by the Commission has expired, making Common Criteria certifications impossible.[1204]

Lastly, it should be noted that the strong involvement of private third parties creates the risk of financial incentives leading to biased assessments. The Medical Devices Directive emphasizes the importance of impartiality[1205] but only prohibits the notified body's director and assessment and verification staff—but not its consultative staff—from being directly involved in the design, construction, marketing or maintenance of the devices.[1206] This potentially creates significant conflicts of interest for notified bodies.[1207] Furthermore, manufacturers of medical devices or secure-signature-creation devices may engage in "forum shopping," thereby creating additional incentives for certifying bodies to lower their requirements.[1208]

[1202] *Cf. also supra* chapter 4.3.4.1 (discussing the eSignature Directive's deficiencies with regard to "trustworthy systems and products" to be used by certification-service-providers).

[1203] *See* supra chapter 4.5.3.

[1204] *See id.*

[1205] *See* Medical Devices Directive annex IX.5 (stating that "[t]he impartiality of the notified body must be guaranteed").

[1206]*See* Medical Devices Directive annex IX.1.

[1207] *Cf.* John Y. Chai, *Medical Device Regulation in the United States and the European Union: A Comparative Study*, 55 FOOD & DRUG L.J. 57, 62 et seq. (2000) (discussing the potential conflicts of interest crated by the utilization of third parties).

[1208] This is an inherent risk of any product evaluation model that allows the manufacturer (instead of the users) to choose the certifying body. ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 878 (2d ed. 2008) (discussing this problem in the context of the Common Criteria).

4.5.4.2. Quality Control v. Quality Assurance

The level of information security offered by software is fundamentally a software quality issue. When attempting to regulate software quality, one of the most fundamental questions is whether to focus on quality control or on quality assurance.

Quality control is a *product-based* approach that attempts to measure and control the quality of the produced products by detecting and correcting defects.[1209] Quality assurance, on the other hand, is a *process-based* approach. It is concerned with the quality of the processes used to create a quality product and attempts to prevent—rather than detect and correct—defects.[1210]

The Quality System Regulation adopted by the FDA put a strong emphasis on quality assurance, in particular by requiring numerous design controls. The FDA's General Principles of Software Validation state that a manufacturer has to "focus on preventing the introduction of defects into the software development process" rather than "trying to 'test quality into' the

[1209] *Cf.* ISO, QUALITY MANAGEMENT SYSTEMS – FUNDAMENTALS AND VOCABULARY, ISO 9000:2005 § 3.2.10 (2005) (defining "quality control" as "part of quality management focused on fulfilling quality requirements"); CARNEGIE MELLON UNIV., CMMI® FOR DEVELOPMENT, VERSION 1.2, at 552 (2006), *available at* http://www.sei.cmu.edu/reports/06tr008.pdf (defining "quality control" as "[t]he operational techniques and activities that are used to fulfill requirements for quality"); INFORMATION SECURITY MANAGEMENT HANDBOOK 3116 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (defining "quality control" as a "[p]rocess by which product quality is compared with standards"); NINA S. GODBOLE, SOFTWARE QUALITY ASSURANCE: PRINCIPLES AND PRACTICE 8 (2004) (emphasizing the product-based corrective approach of quality control).

[1210] *Cf.* ISO, QUALITY MANAGEMENT SYSTEMS – FUNDAMENTALS AND VOCABULARY, ISO 9000:2005 § 3.2.10 (2005) (defining "quality assurance" as "part of quality management focused on providing confidence that quality requirements *will be fulfilled*" (emphasis added)); CARNEGIE MELLON UNIV., CMMI® FOR DEVELOPMENT, VERSION 1.2, at 552 (2006), *available at* http://www.sei.cmu.edu/reports/06tr008.pdf (defining "quality assurance" as "[a] planned and systematic means for assuring management that the defined standards, practices, procedures, and methods of the process are applied"); INFORMATION SECURITY MANAGEMENT HANDBOOK 3116 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (defining "quality assurance" as "[a]n overview process that entails planning and systematic actions to ensure that a project is following good quality management practices"); NINA S. GODBOLE, SOFTWARE QUALITY ASSURANCE: PRINCIPLES AND PRACTICE 8 (2004) (emphasizing the process-based preventive approach of quality assurance). *Cf. also* Joseph M. Juran, *Attaining Superior Results through Quality, in* JURAN'S QUALITY HANDBOOK 33 (Joseph M. Juran & Joseph A. De Feo eds., 6th ed. 2010) (emphasizing that the purpose of quality assurance is to assure *third parties* of the quality of the products) software code after it is written" because "the complexity of most software prevents it from being exhaustively tested," rendering the ability of software testing "very limited […] to surface all latent defects."[1211]

The Medical Devices Directive also stresses the importance of a process-based approach, in particular with regard to software: The essential requirements provide that software must be validated "taking into account the principles of development lifecycle"[1212] and IEC 62304:2006, a reference to which has been published by the Commission, almost exclusively focuses on software development *processes*.[1213]

In stark contrast to the FDA's Quality System Regulation and the Medical Devices Directive, the eSignature Directive implements an approach that is primarily product-based. Annex III of the Directive defines the properties of a particular type of signature product: a secure-signature-creation device. CWA 14169:2002, the technical standard that creates a presumption of compliance for all products that conform to it, does contain some quality assurance elements that establish requirements for the software development process.[1214]

[1211] FDA, GENERAL PRINCIPLES OF SOFTWARE VALIDATION; FINAL GUIDANCE FOR INDUSTRY AND FDA STAFF 11 (2002), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf.

[1212] Medical Devices Directive annex I.12.1a.

[1213] INT'L ELECTROTECHNICAL COMM'N [IEC], MEDICAL DEVICE SOFTWARE – SOFTWARE LIFE CYCLE PROCESSES, IEC 62304:2006, at 11 (2006) ("This standard provides a framework of life cycle PROCESSES with ACTIVITIES and TASKS necessary for the safe design and maintenance of MEDICAL DEVICE SOFTWARE."). Note that commentators have questioned whether medical devices are appropriate for the "New Approach" since they would "not meet the criterion that the product category be sufficiently homogeneous to allow common 'essential requirements' to be defined." Linda R. Horton, *Medical Device Regulation in the European Union*, 50 FOOD & DRUG L.J. 461, 465 (1995). However, a process-based approach largely alleviates this criticism.

[1214] In the terminology used by the Common Criteria, these are referred to as Security Assurance Requirements (SARs). All of the three Protection Profiles (PPs) provided by CWA 14169:2002 contain a number of SARs. *See* CEN, SECURE SIGNATURE-CREATION DEVICES "EAL 4+," CEN WORKSHOP AGREEMENT CWA 14169:2002, at 43, 113, 182 (2002), *available at* http://www.a-sit.at/pdfs/cwa14169.pdf.

However, due to its nature as a product certification standard, CWA 14169:2002 nonetheless primarily focuses on the security properties *of the product*.

The product-based approach of the eSignature Directive becomes even more apparent when considering the security requirements the Directive establishes for signature products that are needed in addition to secure-signature-creation devices to create an electronic signature (e.g. a human interface component): Indeed, the Directive does not establish any requirements for such products. This very well demonstrates that a product-based approach carries the risk of too narrow product definitions that leave important components without any security requirements.

Even more importantly, a product-based approach to software quality faces the fundamental problem that most software products are much too complex to allow a timely and cost-effective evaluation of the level of information security provided by the software.[1215] Evaluations pursuant to the Common Criteria[1216] can be carried out with different levels of rigor, referred to as Evaluation Assurance Levels (EALs) which range from EAL1 ("Functionally Tested") to EAL7 ("Formally Verified Design and Tested").[1217] Commercial software is typically evaluated using EAL4 ("Methodically Designed, Tested, and

[1215] *Cf. supra* chapter 2.3.3 (discussing the reasons for increasingly complex software products).

[1216] The ISO/IEC standard 15408 (commonly known as the Common Criteria) consists of three parts: ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – EVALUATION CRITERIA FOR IT SECURITY – PART 1: INTRODUCTION AND GENERAL MODEL, ISO/IEC 15408-1:2009 (2009); ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – EVALUATION CRITERIA FOR IT SECURITY – PART 2: SECURITY FUNCTIONAL COMPONENTS, ISO/IEC 15408-2:2008 (2008); ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – EVALUATION CRITERIA FOR IT SECURITY – PART 3: SECURITY ASSURANCE COMPONENTS, ISO/IEC 15408-3:2008 (2008).

[1217] *See* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – EVALUATION CRITERIA FOR IT SECURITY – PART 3: SECURITY ASSURANCE COMPONENTS, ISO/IEC 15408-3:2008 § 7.1 (2008).

Reviewed") which does not include a full review of the source code.[1218] To define the security requirements with respect to which a product is to be evaluated using the Common Criteria framework, a Protection Profile has to be drafted.[1219] Protection Profiles often include unrealistic assumptions that drastically narrow the scope of the evaluation.[1220] For example, the Controlled Access Protection Profile[1221] (CAPP) against which many operating systems have been certified,[1222] contains an assumption that effectively disregards that computers may be connected to the Internet (TOE or Target of Evaluation refers to the product)[1223]:

> Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. CAPP-conformant TOEs are applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements which address the need to trust external systems or the communications links to such systems.

Despite these limitations, EAL4 evaluations typically take between nine and 24 months and cost between $150 thousand and $350 thousand.[1224]

[1218] *Cf. id.* § 7.6; ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 874 (2d ed. 2008) (discussing the practical relevance of EALs).

[1219] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – EVALUATION CRITERIA FOR IT SECURITY – PART 1: INTRODUCTION AND GENERAL MODEL, ISO/IEC 15408-1:2009 § 8.3 (2009).

[1220] *Cf.* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 32 (2007) (stating that "the environment assumed by the vendor might have no relationship whatsoever to the customer's actual environment, making the EAL ratings' assurances difficult to translate into the real world").

[1221] NAT'L SEC. AGENCY [NSA], CONTROLLED ACCESS PROTECTION PROFILE, VERSION 1.D (1999), *available at* http://www.niap-ccevs.org/cc-scheme/pp/PP_OS_CA_V1.d.pdf.

[1222] For example, Red Hat Enterprise Linux, Windows Vista, and SUSE Linux Enterprise Server. *See* http://www.commoncriteriaportal.org/products/#OS (last accessed Feb. 10, 2011).

[1223] NAT'L SEC. AGENCY [NSA], CONTROLLED ACCESS PROTECTION PROFILE, VERSION 1.D 16 (1999), *available at* http://www.niap-ccevs.org/cc-scheme/pp/PP_OS_CA_V1.d.pdf.

[1224] *See* GOV'T ACCOUNTABILITY OFFICE [GAO], INFORMATION ASSURANCE—NATIONAL PARTNERSHIP OFFERS BENEFITS, BUT FACES CONSIDERABLE CHALLENGES, GAO-06-392, at 8, 19 (2006), *available at* http://www.gao.gov/new.items/d06392.pdf.

In summary, a product-based regulatory approach requires that the regulatory regime correctly identifies all relevant components and establishes essential requirements for all of these components. The eSignature Directive clearly fails in this regard.

The discussion above also demonstrates that a product-based approach is only viable if the software products to be regulated are not only rather homogenous but also rather simple. A process-based approach is therefore preferable for the regulation of complex software products.

5. Regulating Information Security by Imposing or Limiting Liability

Besides mandating security controls, the second general approach to regulating information security is to allocate liability to various actors of the information security landscape in a way that better aligns risk and risk mitigation capability.[1225] The most obvious approach for allocating liability is to impose it on a certain type of actor, thereby performing a direct risk transfer.[1226]

A less obvious approach is to limit liability. This, too, constitutes a direct risk transfer: Legal instruments other than regulatory intervention can result in a counterproductive risk transfer that intensifies the misalignment between risk and risk mitigation capability.[1227] In this regard, the contractual distribution of risks serves as a prime example: economically powerful parties who would indeed be very capable of mitigating certain risks can use their negotiation power to transfer these risks to another party who may not be capable of mitigating them at all. By limiting such contractually (or otherwise) imposed liability, the counterproductive risk transfer can effectively be reversed, thereby helping to better align risk and risk mitigation capability by restoring the general legal principle of *casum sentit dominus*.

The following chapters discuss regulatory policies that determine the liability of personal information controllers (chapter 5.1), service providers (chapter 5.2), software manufacturers (chapter 5.3), and payment service users (chapter 5.4).

[1225] *Cf. supra* chapter 2.4.4 (discussing the fundamental challenge of the misalignment between risk and risk mitigation capability).

[1226] *See supra* chapter 3.2.3.1.

[1227] *Cf. supra* chapter 2.4.4 (discussing the fundamental challenge of the misalignment between risk and risk mitigation capability).

5.1. Liability of Personal Information Controllers for Breaches of the Security of Personal Information

Making personal information controllers liable for breaches of the security of personal information constitutes a direct risk transfer from the individuals concerned to the personal information controllers.[1228] This chapter analyses the extent to which EU and U.S. law perform such a risk transfer, thereby addressing one of the fundamental challenges of information security: the misalignment between risk and risk mitigation capability.[1229]

5.1.1. Liability under the HIPAA Safeguards Rule

The Health Insurance Portability and Accountability Act of 1996[1230] (HIPAA) (see *supra* chapter 4.1.1) does not provide a private cause of action, thereby effectively shielding covered entities from liability.[1231] However, some state courts have allowed the incorporation of HIPAA as a standard of care in common law tort claims[1232] (cf. *infra* chapter 5.1.5.5).

Furthermore, HIPAA, as amended by the HITECH Act, allows State attorneys general to bring *parens patriae* actions to obtain damages on behalf of the residents of the State if the interest of one or more of the residents "has been or is threatened or adversely affected" by a

[1228] *See* chapter 3.2.3.1 (introducing the regulatory risk treatment option of direct risk transfer).

[1229] *See* chapter 2.4.4.

[1230] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[1231] *See* Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006). *See also* Johnson v. Quander, 370 F. Supp. 2d 79, 100 (D.D.C. 2005), *aff'd*, 440 F.3d 489 (D.C. Cir. 2006). *See* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV 331, 354 (2007) (arguing for a private cause of action to fill the deterrence void left by resource-limited public enforcement efforts). *But cf.* Jack Brill, *Giving HIPAA Enforcement Room to Grow: Why There Should Not (Yet) Be a Private Cause of Action*, 83 NOTRE DAME L. REV. 2105 (2008) (arguing that a private cause of action would significantly increase the overall costs of health care).

[1232] *See* Acosta v. Byrum, 638 S.E.2d 246, 253 (N.C. Ct. App. 2006); Sorensen v. Barbuto, 143 P.3d 295 (Utah Ct. App. 2006), *aff'd*, 177 P.3d 614 (Utah 2008). *Cf.* Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L. J. 617 (2002).

HIPAA violation.[1233] Statutory damages are available in the amount calculated by multiplying the number of violations by up to $100, in total not exceeding $25,000 for all violations of an identical provision during a calendar year.[1234]

However, no damages can be obtained if the failure to comply was not due to willful neglect[1235] and is corrected during a 30-day period beginning on the first date the person liable for the damages knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.[1236]

5.1.2. Liability under the Gramm-Leach-Bliley Act Safeguards Rules

Courts have consistently held that the Gramm-Leach-Bliley Act (GLBA)[1237] (see chapter 4.1.2) does not provide a private right of action.[1238] Commentators suggest, however, that the Safeguards Rules adopted pursuant to GLBA § 501(b), like the HIPAA Security Rule, should inform the standard of care in common law tort claims[1239] (cf. *infra* chapter 5.1.5.5).

[1233] 42 U.S.C. § 1320d-5(d)(1)

[1234] 42 U.S.C. § 1320d-5(d)(2).

[1235] *See* 42 U.S.C. § 1320d-5(b)(2)(A) (referring to 42 U.S.C. § 1320d-5(a)(1)(C).

[1236] *See* 42 U.S.C. § 1320d-5(b)(2)(A).

[1237] Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338. For a general introduction see Bernard Shull, *Banking, commerce and competition under the Gramm-Leach-Bliley Act*, 47 ANTITRUST BULL. 25 (2002). For the history of GLBA see Geoffrey M. Connor, *The Financial Services Act of 1999—The Gramm-Leach-Bliley Act*, 71 PA B. ASSN. Q. 29 (2000). *See also* George W. Arnet, III, *The Death of Glass-Steagall and the Birth of the Modern Financial Services Corporation*, 203 N.J. LAW. 42 (2000) (giving information about the background of the Glass-Steagall Act and its development).

[1238] For a recent decision see *In re* Lentz, 405 B.R. 893, 899 (Bankr. N.D. Ohio 2009) (citing Dunmire v. Morgan Stanley DW Inc., 475 F.3d 956 (8th Cir. 2007); *In re* Southhall, No. 07-00115, 2008 WL 5330001, at *4 (Bankr. N.D. Ala. Dec. 18, 2008); and *In re* French, 401 B.R. 295, 309 (Benkr. E.D. Tenn. 2009)).

[1239] *See* Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who is Going to Pay for It?*, 88 MARQ. L. REV. 847, 865 (2005) (arguing that a violation of the GLBA Safeguard Requirements should allow a negligence per se cause of action); Anthony D. Milewski Jr., *Compliance With California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide*, 2 SHIDLER J. L. COM. & TECH. 19 (2006).

5.1.3. Liability under the Fair Credit Reporting Act

Sections 616[1240] and 617[1241] of the Fair Credit Reporting Act (FCRA)[1242] provide a private cause of action for willful as well as negligent noncompliance with any requirement imposed by FCRA. Regarding the protection of the confidentiality of information, these requirements include the mandatory identification and authentication procedures under FCRA § 607[1243] (see chapter 4.1.3.1), and the Disposal Rules promulgated pursuant to FCRA § 628[1244] (see chapter 4.1.3.2). Regarding the protection of the integrity of information, FCRA imposes the requirements of mandatory procedures to assure accuracy of reported information under FCRA § 697(b)[1245] (see chapter 4.1.3.3), the impersonation fraud "Red Flag" requirements, and the mandatory change of address procedures for card issuers under the Red Flags Rule issued pursuant to FACTA §§ 114 and 315[1246] (see chapters 4.1.3.5 and 4.1.3.6).

A consumer, "with respect to"[1247] whom a willful noncompliance occurred, may claim (1) any actual damages (including immaterial damages)[1248] sustained as a result of the noncompliance

[1240] 15 U.S.C. § 1681n (2010)

[1241] 15 U.S.C. § 1681o (2010).

[1242] Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114 (1970) (codified at 15 U.S.C. § 1681).

[1243] 15 U.S.C. § 1681e.

[1244] 15 U.S.C. § 1681w(a)(1).

[1245] 15 U.S.C. § 1681e(b).

[1246] 15 U.S.C. §§ 1681c(h), 1681m(e).

[1247] A consumer may have standing to sue even where the information at issue does not relate to the consumer but to the consumer's spouse, provided that the information in the file adversely affects the consumer. Koropoulos v. Credit Bureau, Inc., 734 F.2d 37, 46 (D.C. Cir. 1984). *Cf.* CHI CHI WU & ELISABETH DE ARMOND, FAIR CREDIT REPORTING 337 (6th ed. 2006).

[1248] *See, e.g.,* Millstone v. O'Hanlon Reports, Inc., 528 F.2d 829, 834 (8th Cir. 1976) (awarding $2,500 in actual damages for loss of sleep, nervousness, frustration and mental anguish); Dalton v. Capital Associated Indus., Inc., 257 F.3d 409, 418 (holding that damages for emotional distress and loss of reputation are recoverable under FCRA). *Cf.* CHI CHI WU & ELISABETH DE ARMOND, FAIR CREDIT REPORTING 359 (6th ed. 2006).

or statutory damages of not less than $100 and not more than $1,000;[1249] (2) such amount of punitive damages as the court may allow;[1250] and (3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.[1251]

As regards negligent noncompliance, the consumer may only claim actual damages (including immaterial damages) and the costs of the action together with reasonable attorney's fees.[1252] Statutory or punitive damages are not available.[1253]

In this context it should be noted that the FCRA provides consumer reporting agencies, users, and furnishers with a limited immunity for tort liability which was introduced as a quid pro quo[1254] for obligations created by the FCRA to disclose information to consumers.[1255] FCRA § 610(e)[1256] provides that no consumer may bring any action or proceeding "in the nature of defamation, invasion of privacy, or negligence"[1257] with respect to the reporting of information against any consumer reporting agency, any user of information, or any person

[1249] 15 U.S.C. § 1681n(a)(1)(A).

[1250] 15 U.S.C. § 1681n(a)(2).

[1251] 15 U.S.C. § 1681n(a)(3).

[1252] 15 U.S.C. § 1681o.

[1253] *Id.*

[1254] *See* McAnly v. Middleton & Reutlinger, P.S.C., 77 F. Supp. 2d 810, 814 (W.D. Ky. 1999) (stating that § 1681h(e) "is a quid pro quo grant of protection for statutorily required disclosures"); Remarks of Sen. Proxmire, 115 CONG. REC. 33,411 (1969) ("That is the quid pro quo […]").

[1255] *See generally* CHI CHI WU & ELISABETH DE ARMOND, FAIR CREDIT REPORTING 311 et seq. (6th ed. 2006).

[1256] 15 U.S.C. § 1681h(e).

[1257] *Id.* Other torts that are not "in the nature of" of these three torts are not restricted by the immunity. *But see* Harmon v. Regions Bank, 961 So. 2d 693, 698 (Miss. 2007) (holding that a harassment claim is closely affiliated with and can be deemed "in the nature of" an invasion of privacy claim). *Cf. also* CHI CHI WU & ELISABETH DE ARMOND, FAIR CREDIT REPORTING 314 (6th ed. 2006).

who furnishes information to a consumer reporting agency,[1258] based on information that had to be disclosed pursuant to the FCRA,[1259] or based on "information disclosed by a user of a consumer report to or for a consumer against whom the user has taken adverse action, based in whole or in part on the report."[1260] The immunity does, however, not apply if false information is furnished "with malice or willful intent to injure such consumer."[1261]

In addition to a private cause of action, FCRA § 621[1262] also allows any chief law enforcement officer of a State, or an official or agency designated by a State to bring *parens patriae* actions on behalf of the residents of the State to obtain damages for which the defendant is liable to such residents under FCRA § 616 and § 617.[1263]

5.1.4. Liability Under the Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act of 1998 (COPPA)[1264] does not provide any private right of action. However, it allows State attorneys general to bring *parens patriae* actions on behalf of the residents of the State who have been or are threatened or adversely affected by violations of the COPPA Rule.[1265] In particular, State attorneys general may obtain "damage, restitution, or other compensation" on behalf of residents of the State.[1266] It

[1258] Accordingly, a furnisher only enjoys immunity when furnishing information to a consumer reporting agency.

[1259] *See* 15 U.S.C. § 1681g, 1681h, and 1681m.

[1260] 15 U.S.C. § 1681h(e).

[1261] *Id.*

[1262] 15 U.S.C. § 1681s.

[1263] 15 U.S.C. § 1681s(c)(1)(B).

[1264] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2581-728 (1998) (codified at 15 U.S.C. §§ 6501-6506). *Cf. supra* chapter 4.1.4 (discussing COPPA's mandatory safeguard requirements).

[1265] 15 U.S.C. § 6504(a)(1) (2010). *See supra* chapter 4.1.4 (discussing the mandatory safeguard requirements under the COPPA Rule).

[1266] 15 U.S.C. § 6504(a)(1)(C).

has to be noted that COPPA neither addresses whether the liability is fault-based nor does it provide any guidance regarding the question of recoverable damages.[1267]

5.1.5. Liability under California and New York State Law

5.1.5.1. Liability for Violations of SSN Protection Laws

As discussed in chapter 4.1.7.1, California Senate Bill 168[1268] states that any person or entity, not including a state or local agency, must not require an individual to transmit her Social Security number (SSN) over the Internet "unless the connection is secure or the Social Security number is encrypted."[1269] Furthermore an individual must not be required to use her SSN to access a website,[1270] unless "a password or unique personal identification number or other authentication device is also required to access the Web site."[1271]

A violation of Senate Bill 168 constitutes an act of "unfair competition"[1272] which allows an individual "who has suffered injury in fact and has lost money or property as a result of the unfair competition"[1273] to seek orders and judgments "as may be necessary to restore to any person in interest any money or property, real or personal, which may have been acquired by

[1267] In particular, COPPA does not provide any statutory damages.

[1268] 2001 Cal. Legis. Serv. Ch. 720 (S.B. 168) (West) (codified at CAL. CIV. CODE §§ 1785, 1798.85 as amended).

[1269] CAL. CIV. CODE § 1798.85(a)(3) (West 2010).

[1270] *Cf.* Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 916 (N.D. Cal. 2009) (holding that requiring an individual to use his SSN to submit an online job application does not violate CAL. CIV. CODE § 1798.85(a)(4)).

[1271] CAL. CIV. CODE § 1798.85(a)(4).

[1272] *Cf.* CAL. BUS. & PROF. CODE § 17200 (stating that "unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice […]").

[1273] CAL. BUS. & PROF. CODE § 17204. This requirement is established by § 17203 by way of reference to "the standing requirements of Section 17204."

means of such unfair competition."[1274] This constitutes a strict liability regime.[1275] A person who has standing to sue on his own behalf (and complies with California Civil Procedure § 382)[1276] may also bring a class action.[1277] However, the plaintiff may only seek injunctive relieve or restitution of "money or property" but not damages.[1278]

New York General Business Law § 399-dd is almost identical to California's Senate Bill 168.[1279] But like in many other states that have passed SSN protection statutes, no private right of action is available.[1280]

[1274] CAL. BUS. & PROF. CODE § 17203.

[1275] *See* Cortez v. Purolator Air Filtration Products Co., 999 P.2d 706, 717 (Cal. 2000) (holding that California unfair competition law "imposes strict liability when property or monetary losses are occasioned by conduct that constitutes an unfair business practice"); People v. Cappuccio, Inc., 251 Cal. Rptr. 657, 664 (Cal. Ct. App. 1988) (holding that intent is not an element that needs to be proven to establish a violation of section 17200).

[1276] *Cf. infra* chapter 5.1.7.4 (discussing the requirements under CAL. CIV. PROC § 382).

[1277] *See* CAL. BUS. & PROF. CODE § 17203 (stating that "[a]ny person may pursue representative claims or relief on behalf of others only if the claimant meets the standing requirements of Section 17204 and complies with Section 382 of the Code of Civil Procedure"). *Cf.* H. Scott Leviant, *Unintended Consequences: How the Passage of Ballot Proposition 64 May Increase the Number of Successful Wage and Hour Class Actions in California*, 6 U.C. DAVIS BUS. L.J. 183, 186 (2006).

[1278] *See* Korea Supply Co. v. Lockheed Martin Corp., 63 P.3d 937, 943 (Cal. 2003) (holding that an action under CAL. BUS. & PROF. CODE § 17203 is equitable in nature and that damages cannot be recovered); U.S. v. Sequel Contractors, Inc., 402 F.Supp.2d 1142, 1156 (C.D. Cal. 2005) (holding that restitution is limited to the return of property or funds in which the plaintiff has an ownership interest and that damages are not an available remedy under CAL. BUS. & PROF. CODE § 17200 et seq.). *Cf. also* H. Scott Leviant, *Standing Under the Unfair Competition Law is Unlikely to Exist for Competitors,* 50 ORANGE COUNTY LAW. 51, 52 (2008) (discussing Korea Supply Co. v. Lockheed Martin Corp.).

[1279] Note that N.Y. GEN. BUS. LAW § 399-dd(2)(f) (2010), which was enacted in 2008, goes beyond California S.B. 168 by also prohibiting the encoding or embedding of a Social Security number "in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the social security number as required by this section."

[1280] *Cf.* Jonathan J. Darrow & Stephen D. Lichtenstein, *"Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age*, 10 N.C. J.L. & TECH. 1, 43 (2008). *Cf. supra* chapter 4.1.7.1 (discussing that the attorney general may bring an action for an injunction and civil penalties).

5.1.5.2. Liability for Violations of Statutory Disposal Requirements

As discussed in chapter 4.1.7.2, California Assembly Bill 2246[1281] introduced and Assembly Bill 1094[1282] further amended California Civil Code § 1798.81 which mandates that businesses take all reasonable steps to dispose, or arrange for the disposal, of "personal information" by shredding, erasing, or otherwise modifying the personal information to make it unreadable or undecipherable through any means. This provision has a very broad scope as it defines "personal information" very broadly as "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual" not including "publicly available information."[1283]

Any customer[1284] who is injured by a violation of this provision may institute a civil action to recover damages[1285] and to enjoin the business from any further violations.[1286] Note, however, that the statute gives no indication as to what types of damages plaintiffs can recover.[1287]

The corresponding provision under New York law is New York General Business Law § 399-h. However, no private right of action is available.[1288]

[1281] 2000 Cal. Adv. Legis. Serv. 5942 (Deering) (codified at CAL. CIV. CODE §§ 1798.80-82).

[1282] 2009 Cal. Legis. Serv. Ch. 134 (West) (effective as of Jan. 1, 2010).

[1283] CAL. CIV. CODE § 1798.80(e) (West 2010).

[1284] *See* CAL. CIV. CODE § 1798.80(c) (defining "customer" as "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business").

[1285] CAL. CIV. CODE § 1798.84(b).

[1286] CAL. CIV. CODE § 1798.84(e). *Cf.* 5 B.E. WITKIN, SUMMARY OF CALIFORNIA LAW, Torts § 670, at 983 (10th ed. 2005).

[1287] *Cf.* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 266 (2005). No court has yet ruled on this issue.

[1288] *Cf.* chapter 4.1.7.2 (discussing that the attorney general may seek a civil penalty or an injunction).

5.1.5.3. Liability under California Assembly Bill 1950

As discussed in chapter 4.1.7.3, California Assembly Bill 1950[1289] mandates that businesses[1290] that "own or license"[1291] personal information about a California resident (1) "implement and maintain reasonable security procedures and practices appropriate to the nature of the information";[1292] and (2) contractually obligate nonaffiliated third parties to which it discloses information, to implement and maintain "reasonable security procedures and practices."[1293]

Assembly Bill 1950 only covers "personal information" which is narrowly defined as a California resident's name[1294] in combination with: (a) her Social Security number; (b) her driver's license number or California identification card number; (c) her account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (c) medical information.[1295] Assembly Bill 1950 does not cover information that has been lawfully made

[1289] 2004 Cal. Adv. Legis. Serv. 381 (codified at CAL. CIV. CODE § 1798.81.5 (West 2010))

[1290] This includes not-for-profit businesses. CAL. CIV. CODE § 1798.80(a). Businesses that are subject to certain other federal and state statutes are excluded. CAL. CIV. CODE § 1798.81.5(e). *See* chapter 4.1.7.3.

[1291] *See* CAL. CIV. CODE § 1798.81.5(a) (stating that the phrase "owns or licenses" includes, but is not limited to, "personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates").

[1292] CAL. CIV. CODE § 1798.81.5(b).

[1293] CAL. CIV. CODE § 1798.81.5(c). The statute does not expressly require any oversight of the third party.

[1294] First name or first initial in combination with the last name. CAL. CIV. CODE § 1798.81.5(d)(1).

[1295] CAL. CIV. CODE § 1798.81.5(d)(1)(A)-(D). "Medical information" is defined as "individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional." CAL. CIV. CODE § 1798.81.5(d)(2).

available to the general public from federal, state, or local government records[1296] or information that has been "encrypted."[1297]

For violations of Assembly Bill 1950, the same remedies are available as for violations of the disposal requirements under California Civil Code § 1798.81: a customer[1298] who is injured by a violation may institute a civil action to recover damages[1299] and to enjoin the business from any further violations.[1300]

5.1.5.4. Liability Under California Senate Bill 541

California Senate Bill 541[1301] was passed in 2008 and added § 1280.15 to the California Health & Safety Code. This section introduced—in addition to an obligation to notify security breaches which is discussed *infra* in chapter 6.2.2—an obligation for clinics, health facilities, home health agencies, and licensed hospices[1302] to prevent "unlawful or unauthorized access to, and use or disclosure of," patients' medical information.[1303] Violations of this obligation

[1296] CAL. CIV. CODE § 1798.81.5(d)(3). The exclusion of information based on a lack of confidentiality interest is somewhat inconsistent as A.B. 1950 does not only protect the confidentiality but also the integrity and availability of information.

[1297] CAL. CIV. CODE § 1798.81.5(d)(1). It has to be noted that the statute does not provide any indication as to the required strength of the encryption.

[1298] *See* CAL. CIV. CODE § 1798.80(c) (defining "customer" as "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business").

[1299] CAL. CIV. CODE § 1798.84(b).

[1300] CAL. CIV. CODE § 1798.84(e). *Cf.* 5 B.E. WITKIN, SUMMARY OF CALIFORNIA LAW, Torts § 669, at 982 (10th ed. 2005).

[1301] 2008 Cal. Legis. Serv. Ch. 605 (West).

[1302] CAL. HEALTH & SAFETY CODE § 1280.15(b) (West 2010) only covers hospices that are licensed pursuant to CAL. HEALTH & SAFETY CODE §§ 1204, 1250, 1725, or 1745.

[1303] *See* CAL. HEALTH & SAFETY CODE § 1280.15(a) (West 2010). *See* CAL. CIV. CODE § 56.05(g) (defining "medical information" as "individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment"). "Individually identifiable" is defined as including or containing "any element of personal identifying information sufficient to allow are subject to administrative penalties by the California Department of Public Health (hereinafter *CDPH*).[1304]

Since the statute provides that covered entities should fulfill their duty “consistent with Section 130203” of the California Health and Safety Code which refers to the implementation of “*appropriate* administrative, technical, and physical safeguards,”[1305] it is clear that California Senate Bill 541 does not impose liability for all possible security breaches.[1306] Liability essentially only attaches where a lack of reasonable safeguards was the proximate cause of the breach. However, whether a covered entity failed to implement reasonable safeguards due to negligence is immaterial, making California Senate Bill 541 a strict liability regime.

Senate Bill 541 does not provide a private right of action. However, the CDPH may assess administrative penalties of up to $25,000 per affected patient, and up to $17,500 per subsequent occurrence of a breach.[1307] It has to be emphasized that a covered entity may only be liable for penalties if a security breach actually occurs—and not solely based on a failure to implement appropriate safeguards. Despite the lack of a private right of action, California Health and Safety Code § 1280.15 is therefore best described as a liability regime.

identification of the individual […] or other information that, alone or in combination with other publicly available information, reveals the individual’s identity.” *Id.*

[1304] Note that CAL. HEALTH & SAFETY CODE § 1280.15(b) does not require the regulated entities to implement any security controls, it “only” makes them liable for administrative penalties should a data breach occur. It is for this reason, that this provision is discussed here and not in chapter 4.1.

[1305] CAL. HEALTH & SAFETY CODE § 130203(a) (emphasis added).

[1306] *Cf.* Stephen Wu, *California Health Care Data Protection Law Addresses Worker Snooping*, RSA CONFERENCE BLOG, Apr. 12, 2009, https://365.rsaconference.com/blogs/ediscovery/2009/04.

[1307] CAL. HEALTH & SAFETY CODE § 1280.15(a).

5.1.5.5. Common Law Tort Liability

The above-discussed statutory liabilities constitute very significant steps towards ensuring accountability of personal information controllers. However, these statutory liabilities are limited in a number of ways: California Senate Bill 168 and New York General Business Law § 399-dd apply exclusively to Social Security numbers (see chapter 5.1.5.1), California Civil Code § 1798.81 applies to a vide range of personal information but only addresses disposal requirements (see chapter 5.1.5.2); and California Assembly Bill 1950 generally requires "reasonable security procedures" but is limited to certain types of personal information (see chapter 5.1.5.3). Common law causes of action, specifically the tort of negligence and the tort of public disclosure of private facts, are therefore of great practical importance.

Negligence is a tort that can be defined as "[t]he failure to exercise the standard of care that a reasonably prudent person would have exercised in a similar situation."[1308]

To prevail in court, a plaintiff has to establish four elements: (1) the presence of a duty; (2) the breach of that duty by failing to act "reasonably"; (3) proximate causation;[1309] and (4)

[1308] BLACK'S LAW DICTIONARY 1133 (9th ed. 2009). *Cf.* CAL. CIV. CODE § 1714(a) (stating that "[e]veryone is responsible, not only for the result of his or her willful acts, but also for an injury occasioned to another by his or her want of ordinary care or skill in the management of his or her property or person, except so far as the latter has, willfully or by want of ordinary care, brought the injury upon himself or herself.").

[1309] *Cf.* Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005) (holding that plaintiff could not prove that the defendant's data breach was the proximate cause of the identity theft), *rev'd and remanded,* 254 Fed.Appx. 664, 667 (9th Cir. 2007) (holding that, to survive summery judgment, plaintiff need not show that the breach was the sole cause of the identity fraud incidents, only that it was, more likely than not, a "substantial factor in bringing about the result"). *Cf.* Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, FED. LAW., Sept. 2007, at 39, *available at* 54-SEP Fed. Law. 39, 42 (Westlaw).

damages that are legally compensable.[1310] As discussed below, in particular the first, second, and fourth element raise a number of unanswered questions.

Under common law, a person generally does not have an affirmative duty to act to protect a third party.[1311] When considering the existence of a duty in a given case, courts usually consider a number of factors: the foreseeability of harm to the plaintiff; the degree of certainty that the plaintiff suffered injury; the closeness of the connection between the defendant's conduct and the injury suffered; the moral blame attached to the defendant's conduct; the policy of preventing future harm; the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach; and the availability, cost, and prevalence of insurance for the risk involved.[1312]

The factor often considered a *conditio sine qua non* is foreseeability of harm to the plaintiff.[1313] Whether a particular accident or malicious action was a "risk reasonably to be perceived"[1314] will greatly depend on the particular facts of the case. However, the general rule that a person is not obligated to anticipate intentional misconduct by third parties,[1315] would not apply where the court finds that the "actor acts with knowledge of peculiar

[1310] *See, e.g.,* United States Liab. Ins. Co. v. Haidinger-Hayes, Inc., 463 P.2d 770, 774 (Cal. 1920); Becker v. Schwartz, 386 N.E.2d 807, 811 (N.Y. 1978). *Cf.* RESTATEMENT (SECOND) OF TORTS § 281 (1965).

[1311] RESTATEMENT (SECOND) OF TORTS § 314 (1965).

[1312] *See* Thompson v. County of Alameda, 614 P.2d 728, 733 (Cal. 1980) (citing Rowland v. Christian, 443 P.2d 561, 564 (Cal. 1968)). *Cf.* Di Ponzio v. Riordan, 679 N.E.2d 616, 618 (N.Y. 1997) (stating that courts consider "whether the relationship of the parties is such as to give rise to a duty of care"; whether "the plaintiff was within the zone of foreseeable harm"; and whether "the accident was within the reasonably foreseeable risks").

[1313] *See* Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 100 (N.Y. 1928) (holding that "[t]he risk reasonably to be perceived defines the duty to be obeyed, and risk imports relation"); Weirum v. RKO General, Inc., 539 P.2d 36, 39 (Cal. 1975) (holding that foreseeability of risk is a primary consideration in establishing element of duty of due care);

[1314] Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 100 (N.Y. 1928).

[1315] RESTATEMENT (SECOND) OF TORTS § 302B cmt. d (1965).

conditions which create a high degree of risk of intentional misconduct."[1316] It has therefore been argued that, due to the insecurity of software and the high frequency of attacks, many security breaches indeed are foreseeable.[1317]

In ultimately deciding on the existence of a duty, courts often also consider whether there is a preexisting relationship between the parties. In this regard, various analogies have been proposed.[1318] However, so far, courts have been rather reluctant to impose an affirmative duty to protect the security of personal information.[1319]

The second element a plaintiff has to establish is a breach of this duty by failing to act "reasonably." What would a "reasonably prudent person in the same or similar circumstances"[1320] do to protect the security of personal data? This question raises many

[1316] RESTATEMENT (SECOND) OF TORTS § 302B cmt. e(H) (1965).

[1317] *See* Meiring de Villiers, *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, 30 HASTINGS COMM. & ENT. L.J. 419, 448 et seq. (2008) (proposing a numerical metric for calculating the risk that a particular unpatched security vulnerability will be successfully exploited); Derek A. Bishop, *To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?*, 3 SHIDLER J. L. COM. & TECH. 7 (2006) (arguing for the general foreseeability of data theft); Jane Strachan, *Cybersecurity Obligations*, 20 MAINE B. J. 90, 91 (2005); Kimberly Kiefer & Randy V. Sabett, *Openness of Internet Creates Potential for Corporate Information Security Liability*, 7 ELECTRONIC COM. & L. REP. 594 (2002); Erin Kenneally, *The Byte Stops Here: Duty and Liability for Negligent Internet Security*, 16 COMPUTER SECURITY J. 1, 20 (2000), *available at* http://web.archive.org/web/20040623113244/http://www.allasso.pt/base/docs/11022984657.pdf; Alan Charles Raul et al., *Liability for Computer Glitches and Online Security Lapses*, 6 ELECTRONIC COM. & L. REP. 849 (2001).

[1318] *See* Kimberly Kiefer & Randy V. Sabett, *Openness of Internet Creates Potential for Corporate Information Security Liability*, 7 ELECTRONIC COM. & L. REP. 594 (2002) (proposing to treat a data subject/service provider relationship analogous to a landlord/tenant relationship); Alan Charles Raul et al., *Liability for Computer Glitches and Online Security Lapses*, 6 ELECTRONIC COM. & L. REP. 849 (2001). *Cf.* KIMBERLY KIEFER ET AL., INFORMATION SECURITY: A LEGAL, BUSINESS, AND TECHNICAL HANDBOOK 39 (2004).

[1319] *See* KIMBERLY KIEFER ET AL., INFORMATION SECURITY: A LEGAL, BUSINESS, AND TECHNICAL HANDBOOK 39 (2004). *But see* Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1008 (N.H. 2003) (woman was killed by stalker who bought the victim's address and Social Security number from the plaintiff, an Internet-based investigation service; the court held that the plaintiff had a duty to exercise reasonable care in disclosing information); Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007) (holding that bank had common law duty to verify the authenticity and accuracy of a credit account application before issuing a credit card irrespective of whether the parties had a prior business relationship).

[1320] Often referred to as the standard of "a reasonable person." *Cf.* RESTATEMENT (SECOND) OF TORTS § 283 (1965).

uncertainties as the answer depends on many factors that change over time and vary from organization to organization: amount and nature of information processed; the graveness of man-made and natural threats to the security of the information; the number and the motivation of potential threat agents; and the size of the organization.[1321] Avoiding these questions, some commentators have suggested that the HIPAA Security Rule and GLBA Safeguards Rules should be used as, or at least inform, the standard of care.[1322] At least two courts have followed that approach.[1323]

Lastly, the type of legally compensable damages constitutes a major obstacle for individuals seeking redress after a security breach. Under the economic loss doctrine, a plaintiff can generally not recover any damages for negligently inflicted "pure economic loss" when the loss does not follow from physical injury or property damage.[1324] As individuals affected by a security breach typically do not suffer physical injury or property damages, their economic

[1321] Trade practice might inform the necessary duty of care. However, as Justice Holmes stated in Texas & Pac. Ry. Co. v. Behymer, 189 U.S. 468, 470 (1903), "[w]hat usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not." *Cf.* KIMBERLY KIEFER ET AL., INFORMATION SECURITY: A LEGAL, BUSINESS, AND TECHNICAL HANDBOOK 39 (2004). Some courts turned to HIPPA for setting the standard of care. *See* Acosta v. Byrum, 638 S.E.2d 246, 253 (N.C. Ct. App. 2006). *Cf.* Denis T. Rice, *Increased Civil Litigation Over Privacy and Security Breaches*, 902 PLI/PAT 149, 168 (2007).

[1322] *See* Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who is Going to Pay for It?*, 88 MARQ. L. REV. 847, 865 (2005) (arguing that a violation of the GLBA Safeguard Requirements should allow a negligence per se cause of action); Anthony D. Milewski Jr., *Compliance With California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide*, 2 SHIDLER J. L. COM. & TECH. 19 (2006). Regarding HIPAA, compare Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L. J. 617 (2002).

[1323] Guin v. Brazos Higher Educ. Serv. Corp., 2006 U.S. Dist. LEXIS 4846, at *8 (D. Minn. 2006) (stating that "in some negligence cases […] a duty of care may be established by statute" and applying GLBA to establish the duty of care, but holding that there was not a breach of that duty in the case). Regarding HIPAA, see Acosta v. Byrum, 638 S.E.2d 246, 253 (N.C. Ct. App. 2006) (allowing HIPAA to be used as evidence of the duty of care). *Cf. also* Sorensen v. Barbuto, 143 P.3d 295 (Utah Ct. App. 2006), *aff'd*, 177 P.3d 614 (Utah 2008).

[1324] *Cf.* San Francisco Unified School Dist. v. W.R. Grace & Co., 44 Cal. Rptr. 2d 305, 310 (Cal. Ct. App. 1995) (holding that until physical injury occurs—until damage rises above the level of mere economic loss—a plaintiff cannot state a cause of action for negligence). *See generally* Robert L. Rabin, *Tort Recovery for Negligently Inflicted Economic Loss: A Reassessment,* 37 STAN. L. REV. 1513 (1985).

losses are generally not recoverable, absent a "special relationship"[1325] with the plaintiff.[1326] This is exemplified by one of the biggest data security breaches which was suffered by TJX Companies, Inc. and affected more than 45 million debit and credit card accounts.[1327] TJX decided to resolve much of the ensuing litigation through settlements.[1328] However, those cases that did make it to judgment on preliminary matters were dismissed in application of the economic loss doctrine.[1329]

[1325] *See* Greystone Homes, Inc. v. Midtec, Inc., 86 Cal. Rptr. 3d 196, 222 (Cal. Ct. App. 2008), where the court considered the following factors: "(1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct, and (6) the policy of preventing future harm" (citing J'Aire Corp. v. Gregory, 598 P.2d 60, 63 (Cal. 1979)).

[1326] *See, e.g.,* Banknorth, N.A. v. BJ's Wholesale Club, Inc., 442 F. Supp. 2d 206, 214 (M.D. Pa. 2006) (dismissing the negligence claim in application of the economic loss doctrine and finding that there was no "special relationship" between the defendants, who's compromised computer systems held debit-card numbers of the plaintiff's customers, and the plaintiff, a bank, who had to issue new cards after the breach); Pa. State Employees Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 326 (M.D. Pa. 2005), *aff'd,* 533 F.3d 162 (3rd Cir. 2008); Sovereign Bank v. BJ's Wholesale Club, Inc., 427 F. Supp. 2d 526, 533 (M.D. Pa. 2006), *aff'd,* 533 F.3d 162, 175 (3rd Cir. 2008); Hendricks v. DSW Shoe Warehouse Inc., 444 F. Supp. 2d 775, 783 (W.D. Mich.) (dismissing action to recover credit monitoring costs due to economic loss doctrine). For a discussion of *Banknorth*, *Pa. State Employees Credit Union*, and *Sovereign Bank* see Kirk J. Nahra, *What Every Litigator Needs to Know About Privacy*, 902 PLI/PAT 277 (2007) and Denis T. Rice, *Increased Civil Litigation Over Privacy and Security Breaches*, 902 PLI/PAT 149 (2007). *See also* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 296 et seq. (2005) (extensively discussing the economic loss doctrine in the context of cybersecurity cases); Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDIS. L.J. 63, 112 (2001).

[1327] The compromise seems to have been possible, in part, due to the use of an outdated wireless network encryption technology used in one of TJX's stores. *See* Dan Kaplan, *TJX breach began in Minnesota Marshalls parking lot*, SC MAGAZINE, May 4, 2007, http://www.scmagazineus.com/report-tjx-breach-began-in-minnesota-marshalls-parking-lot/article/34954/.

[1328] *See* Rick Valliere & Donald G. Aplin, *Identity Theft: TJX Settles Consumer Class Breach Claims; Bank Class Actions Against Retailer Continue*, 12 ELECTRONIC COM. & L. REP. 905 (2007); Bureau of Nat'l Affairs, *TJX, Financial Institution Plaintiffs Settle Claims in Breach of 46 Million Credit Cards*, 14 ELECTRONIC COM. & L. REP. 1296 (2009).

[1329] *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498 (1st Cir. 2009) (applying Massachusetts law). *Cf.* Edward A. Morse & Vasant Raval, *PCIDSS and the Legal Framework for Security: An Update on Recent Developments and Policy Directions,* 1 LYDIAN PAYMENTS J. 31, 33 (2010). For a similar case that affected 4.2 million people see In re Hannaford Bros. Co. Customer Data Security Breach Litigation, 4 A.3d 492, 496 (Me. 2010) (holding that time and effort alone, spent in a reasonable effort to avoid or remediate reasonably foreseeable harm, was not a cognizable injury for which damages could be recovered under law of negligence in action by grocery store customers, whose electronic payment data was allegedly stolen by third-party wrongdoers, against grocer for negligence).

The many uncertainties surrounding the elements of duty, breach, and damages lead to the conclusion that the tort of negligence, as it stands today, hardly results in any significant transfer of risk from the individuals concerned to personal information controllers.[1330]

The second tort to be briefly considered here is the tort of public disclosure of private facts, which is one of the four privacy torts[1331] accepted by most states, including California.[1332] However, it has to be emphasized that this tort is not recognized in the state of New York.[1333] Its elements are (1) public disclosure (2) of a private fact (3) which would be offensive and

[1330] *Cf.* Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information, in* SECURING PRIVACY IN THE INTERNET AGE 111, 128 (Anupam Chander et al. eds., 2008) (stating in conclusion that "[t]he law of torts will need some creativity and development to be used as a device to induce lasting change in security practices"); Kirk J. Nahra, *What Every Litigator Needs to Know About Privacy*, 902 PLI/PAT 277, 281 (2007) (naming the difficulty of proving recoverable damages as one of the major reasons for why there has not been more litigation surrounding security breaches); *Cf. also* KIMBERLY KIEFER ET AL., INFORMATION SECURITY: A LEGAL, BUSINESS, AND TECHNICAL HANDBOOK 39 (2004).

[1331] *Cf. supra* chapter 2.2.1 (discussing the four privacy torts).

[1332] *See* Melvin v. Reid, 297 P. 91, 93 (Cal. Ct. App. 1931) ("In the absence of any provision of law we would be loath to conclude that the right of privacy […] exists in California. We find, however, that the fundamental law of our state contains provisions which, we believe, permit us to recognize the right to pursue and obtain safety and happiness without improper infringements thereon by others"). *Cf.* 5 B.E. WITKIN, SUMMARY OF CALIFORNIA LAW, Torts § 664, at 973 (10th ed. 2005).

[1333] Delan v. CBS, Inc., 458 N.Y.S.2d 608, 612 (N.Y. App. Div. 1983) ("At common law, a cause of action for violation of the right of privacy is not cognizable in this State […], and exists solely by virtue of the statutory provisions of [§§ 50, 51] Civil Rights Law"). N.Y. CIV. RIGHTS LAW § 50 (McKinney 2010) provides that the use of the name, portrait or picture of any living person for the purposes of advertising or trade—without having first obtained her written consent—constitutes a misdemeanor.

objectionable to the reasonable person and (4) which is not of legitimate public concern.[1334] Recoverable damages include pure economic loss as well as immaterial damages.[1335]

The public disclosure element requires that the information "be widely published and not confined to a few persons or limited circumstances."[1336] This drastically limits the applicability of this tort with regard to security breaches as they typically do not lead to personal information being shared with the public at large.[1337] Therefore, the tort of public disclosure of private facts also does not result in a significant risk transfer.

5.1.6. Liability under the EU Data Protection Directive

EUDPD article 23(1) requires Member States to provide that "any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered." However, according to EUDPD article 23(2),

[1334] Diaz v. Oakland Tribune, Inc., 188 Cal. Rptr. 762, 768 (Cal. Ct. App. 1983). *Cf.* RESTATEMENT (SECOND) OF TORTS § 652D (1965). Note the absence of a fault requirement under California law. However, a dictum of the Supreme Court in *Florida Star* may serve as a basis for establishing a fault requirement. *See* The Florida Star v. B.J.F., 491 U.S. 524, 539 (1989) (noting that the lack of a fault or scienter requirement would "[engender] the perverse result that truthful publications challenged pursuant to this cause of action are less protected by the First Amendment than even the least protected defamatory falsehoods"). For a critical perspective see Patrick J. McNulty, *The Public Disclosure of Private Facts: There Is Life After Florida Star*, 50 DRAKE L. REV. 93, 112 (2001) (stating that "the Court failed to note the obvious distinction between the two torts; in defamation, a defendant's fault pertains to the objectively verifiable standard of falsity, whereas in privacy disclosure actions, falsity is irrelevant").

[1335] *See* RESTATEMENT (SECOND) OF TORTS § 652H (1965) (stating that the privacy torts allow the recovery of damages for: (a) the harm to the plaintiff's interest in privacy resulting from the invasion; (b) the plaintiff's mental distress proved to have been suffered if it is of a kind that normally results from such an invasion; and (c) special damage of which the invasion is a legal cause).

[1336] Hill v. National Collegiate Athletic Assn., 865 P.2d 633, 649 (Cal. 1994). *Cf.* RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1965) (stating that "publicity" means that "the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge").

[1337] *Cf. also* Sharona Hoffman & Andy Podgurski, *Information Security of Health Data, in* HARBORING DATA: INFORMATION SECURITY LAW AND THE CORPORATION 103, 109 (Andrea M. Matwyshyn ed., 2009).

Member States may exempt a controller from this liability, in whole or in part, if "he proves that he is not responsible for the event giving rise to the damage."

This liability regime is applicable to the issue of liability for security breaches because the processing of personal data has to be considered "unlawful" if the security measures required by EUDPD article 17[1338] have not been implemented.[1339] Furthermore, the legislative history even suggests that article 23 was specifically created to address the issue of security breaches. In the Commission's amended proposal, article 23(2) still explicitly referred to article 17 ("Security of processing").[1340]

Since the Directive neither defines the term "damages" nor clarifies what it means to be "responsible for the event giving rise to the damage," the scope of recoverable damages as well as the nature of the liability has been the subject of great debate in the literature.

In particular the question of whether immaterial damages should be covered by article 21(1) has been hotly debated. Since the Directive does not define the term—despite a long catalogue of definitions in article 2—and makes no explicit reference to immaterial damages, it has been argued that "damages" should be read to only include material damages.[1341]

[1338] *See* chapter 4.1.8.

[1339] *See* TIMOLEON KOSMIDES, ZIVILRECHTLICHE HAFTUNG FÜR DATENSCHUTZVERSTÖẞE [CIVIL LIABILITY FOR DATA PROTECTION VIOLATIONS] 100 (2010); ILONA KAUTZ, SCHADENERSATZ IM EUROPÄISCHEN DATENSCHUTZRECHT [INDEMNIFICATION UNDER EUROPEAN DATA PROTECTION LAW] 141 (2006).

[1340] *See Amended Commission proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, at 102, COM (1992) 442 final (Oct. 15, 1992). *Cf. also id.* at 55 (recital 24 of the proposed directive also states that a controller may only be exempted from liability "if he proves that he has taken suitable security measures").

[1341] *See* Horst Ehmann & Holger Sutschet, *EU-Datenschutzrichtlinie – Umsetzungsbedarf und Auswirkungen aus der Sicht des Arbeitsrechts* [*EC Data Protection Directive – Needed Transposition and Effects from a Labor Law Perspective*], 1997 RECHT DER DATENVERARBEITUNG 3, 13 (F.R.G.); EUGEN EHMANN & MARCUS HELFRICH, EG-DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE] art. 23 cmt. 27 (1999); Jochen Schneider, *Die EG-Richtlinie zum Datenschutz* [*The EC Directive About Data Protection*], 1993 COMPUTER UND RECHT 35, 35 (F.R.G.); CHRISTIAN BORN, SCHADENSERSATZ BEI DATENSCHUTZVERSTÖẞEN. EIN ÖKONOMISCHES

However the dual purpose of the Directive—the protection of the fundamental right to privacy[1342] and the harmonization of laws in order to enable a free flow of personal data between Member States[1343]—has been used as a strong argument for an extensive interpretations of “damages.”[1344] However, since the ECJ has not yet decided on the issue, it remains unresolved.

As regards the nature of the liability, the wording of article 23 does not make it clear whether Member States should introduce a fault-based liability regime or one that is independent of the tortfeasor’s culpability (i.e. strict liability).[1345] Any attempt to clarify the nature of the liability should also take article 23(2) in consideration.

INSTRUMENT DES DATENSCHUTZES UND SEINE PRÄVENTIVE WIRKUNG [INDEMNIFICATION IN THE CASE OF DATA PROTECTION VIOLATIONS. AN ECONOMIC INSTRUMENT OF DATA PROTECTION AND ITS PREVENTIVE EFFECT] 84 (2001).

[1342] *See* EUDPD art. 1(1) (stating as the Directive’s first objective that “Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data”).

[1343] *See* EUDPD art. 1(2) (stating as the Directive’s second objective that “Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1”).

[1344] For extensive discussions of the interpretation of “damages” within the context of art. 23 and, in particular, why the Directive’s objective requires the inclusion of immaterial damages see TIMOLEON KOSMIDES, ZIVILRECHTLICHE HAFTUNG FÜR DATENSCHUTZVERSTÖßE [CIVIL LIABILITY FOR DATA PROTECTION VIOLATIONS] 101 (2010) and ILONA KAUTZ, SCHADENERSATZ IM EUROPÄISCHEN DATENSCHUTZRECHT [INDEMNIFICATION UNDER EUROPEAN DATA PROTECTION LAW] 163 et seq. (2006). *See also* ULRICH DAMMANN & SPIROS SIMITIS, EG-DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE] art. 23 cmt. 5 (1997); Ulf Brühann & Thomas Zerdick, *Umsetzung der EG-Datenschutzrichtlinie* [*Transposition of the EC Data Protection Directive*], 1996 COMPUTER UND RECHT 429, 435 (F.R.G.); Ulrich Würmeling, *Datenschutz für die Europäische Informationsgesellschaft* [*Data Protection for the European Information Society*], 1995 NEUEN JURISTISCHEN WOCHENSCHRIFT – COMPUTERREPORT 111, 113 (F.R.G.); Ferdinand Kopp, *Das EG-Richtlinienvorhaben zum Datenschutz – Geänderter Vorschlag der EG-Kommission für eine „Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“* [*The EC Directive Proposal About Data Protection—Amended Commission Proposal for an “amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data“*], 1993 RECHT DER DATENVERARBEITUNG 1, 8 (F.R.G.).

[1345] *Cf.* TIMOLEON KOSMIDES, ZIVILRECHTLICHE HAFTUNG FÜR DATENSCHUTZVERSTÖßE [CIVIL LIABILITY FOR DATA PROTECTION VIOLATIONS] 88 (2010) (also noting that it would be incorrect to classify art. 23’s liability regime as *Gefährdungshaftung*, since liability under art. 23 requires not only damages and causation but also the illegality of the actions that cause the damages).

Article 23(2) allows Member States to provide exemptions if the controller can prove that "he is not responsible for the event giving rise to the damage." While this could refer to the controller having to prove his lack of culpability—which would move article 23(1) closer to fault-based liability—it could also be read as requiring the controller to disprove other factors.

In this regard EUDPD recital 55 is relevant which states that Member States may provide an exemption from liability "in particular in cases where [the controller] establishes fault on the part of the data subject or in case of force majeure." Since recital 55 does not explicitly refer to the controller's culpability, it has been argued that article 23(1) and (2), when read together, should be construed as requiring Member States to introduce a liability regime that is independent of the tortfeasor's culpability.[1346] However, the list of cases in recital 55 is non-exhaustive and the concept of *force majeure* is indeed inherently based on due care.[1347] Recital 55 therefore does not provide any strong guidance for how to interpret article 23(2).

Accordingly, it has been argued that a Member State could transpose article 23(1) by implementing a fault-based liability regime.[1348] Others argue that a fault-based liability regime could only be introduced based on EUDPD article 23(2) but not on article 23(1). This

[1346] ILONA KAUTZ, SCHADENERSATZ IM EUROPÄISCHEN DATENSCHUTZRECHT [INDEMNIFICATION UNDER EUROPEAN DATA PROTECTION LAW] 163, 183 (2006).

[1347] *See* Case C-334/08, Commission v. Italy, § 46 (stating that *force majeure* must generally be understood "in the sense of abnormal and unforeseeable circumstances, outside the control of the party relying thereupon, the consequences of which, *in spite of the exercise of all due care, could not have been avoided*" (emphasis added)). *See also, e.g.,* Case 145/85 Denkavit België NV v. Belgium, 1987 E.C.R. 565, § 11; Case C-105/02, Commission v. Germany, 2006 E.C.R. I-9659, § 89; Case C‑377/03, Commission v. Belgium 2006 E.C.R. I‑9733, § 95.

[1348] *See* TIMOLEON KOSMIDES, ZIVILRECHTLICHE HAFTUNG FÜR DATENSCHUTZVERSTÖẞE [CIVIL LIABILITY FOR DATA PROTECTION VIOLATIONS] 89 (2010); Jochen Schneider, *Die EG-Richtlinie zum Datenschutz* [*The EC Directive About Data Protection*], 1993 COMPUTER UND RECHT 35, 35 (F.R.G.).

means that the controller would have to bear the burden of prove regarding (the lack of) his culpability.[1349]

Similarly to the question of the construction of the term "damages," a lot of uncertainty remains with regard to the legal nature of the liability because the ECJ has, so far, not addressed the issue.[1350]

When applying article 23 to the issue of security of processing, an interesting question arises: What relevance does it have that recital 55 allows Member States to provide liability exceptions in cases of *force majeure*? According to established case law of the ECJ, *force majeure* must generally be understood "in the sense of abnormal and unforeseeable circumstances, outside the control of the party relying thereupon, the consequences of which, in spite of the exercise of all due care, could not have been avoided."[1351] In the context of the security of processing of personal data, this means that a controller would have to prove, *inter alia*, that he had exercised due care by implementing all appropriate security measures as required under EUDPD article 17. This is significant because information—in contrast to physical assets—*can* indeed be protected from most of the threats that are traditionally considered *force majeure* (e.g. floods or earthquakes) if reasonable security measures are implemented pursuant to article 17.

[1349] ULRICH DAMMANN & SPIROS SIMITIS, EG-DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE], art. 23 cmt. 6 and 9 (1997).

[1350] For an overview of how the Member States transposed art. 23 see DOUWE KORFF, EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE—COMPARATIVE SUMMARY OF NATIONAL LAWS 179 (2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf.

[1351] *See* Case C-334/08, Commission v. Italy, § 46. *See also, e.g.,* Case 145/85 Denkavit België NV v. Belgium, 1987 E.C.R. 565, § 11; Case C-105/02, Commission v. Germany, 2006 E.C.R. I-9659, § 89; Case C‑377/03, Commission v. Belgium 2006 E.C.R. I‑9733, § 95.

For example, unlike a physical server which stores certain information, the confidentiality, integrity, or availability of that information does not have to be negatively affected if the building which houses the server is destroyed by an earthquake. If, for the purpose of redundancy, the information was replicated onto a remote server, the destruction of the first server may have no effect on the security, in particular the integrity and availability of the information.[1352]

Thus, cases of *force majeure* are much rarer with regard to information assets than they are with regard to physical assets. In this regard, it is noteworthy that, the Commission's amended proposal did not refer to *force majeure*. It captured the circumstances under which liability exemptions should be permissible in a much clearer way: "only if [the controller] proves that he has taken suitable security measures."[1353] Unfortunately, the Council did not follow this approach and chose the wording that can now be found in EUDPD recital 55.[1354] However, under the open wording of article 23(2), Member States can still adopt an exemption like the one that had been included the Commission's amended proposal.

5.1.7. Comparative Assessment

Regulatory policies that hold personal information controllers liable for breaches of the security of personal information have the potential to better align risk and risk mitigation

[1352] For a discussion of data replication techniques see for example EVAN MARCUS & HAL STERN, BLUEPRINTS FOR HIGH AVAILABILITY 433 et seq. (2003).

[1353] *Amended Commission proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, at 55, COM (1992) 442 final (Oct. 15, 1992).

[1354] *See* Council Common Position (EC) No. 1/1995 of 20 Feb. 1995, recital 55, 1995, O.J. (C 93) 1 (stating that a controller may be exempted from liability "if he proves that he is not responsible for the damage, in particular in cases where he reports an error on the part of the data subject or in a case of force majeure").

capability[1355] by directly transferring risk from the individuals concerned to the information controllers.[1356] However, the extent to which a regulatory policy can fulfill this potential depends on (1) the types of recoverable damages (see chapter 5.1.7.1); (2) the availability of statutory damages (see chapter 5.1.7.2); (3) the nature of the liability (see chapter 5.1.7.3); and (4) the availability of class actions and *parens patriae* actions (see chapters 5.1.7.4 and 5.1.7.5).

At the outset of this assessment is has to be emphasized that liability for security breaches may not exclusively be imposed by means of a private right of action. HIPAA and COPPA instead provide *parens patriae* actions while California Senate Bill 541 only provides administrative penalties.

GLBA, California's SSN protection law, New York's SSN protection law, and New York's statutory disposal requirements do not allow the recovery of damages (whether by means of a private or public action). Accordingly, they do not perform any risk transfer and will be excluded from the following discussion.[1357]

[1355] *See* chapter 2.4.4 (identifying the misalignment between risk and risk mitigation capability as one of the fundamental challenges of information security).

[1356] *See* chapter 3.2.3.1 (introducing the concept of a direct risk transfer).

[1357] *See supra* chapter 5.1.2 (discussing the lack of a private right of action under GLBA); chapter 5.1.5.1 (discussing the lack of a private right of action under New York's SSN protection law); chapter 5.1.5.2 (discussing the lack of a private right of action under New York's statutory disposal requirements); chapter 5.1.5.2 (discussing California's SSN protection law which does provide a private right of action; however it is equitable in nature and therefore does not allow the recovery of damages).

5.1.7.1. Recoverability of Purely Economic Losses and Immaterial Damages

Breaches of the security of personal information sometimes cause physical damages or physical injuries.[1358] However, in the vast majority of cases, they only cause purely economic losses or immaterial damages.[1359] Whether these types of damages can be recovered is therefore of significant practical importance.

The only two liability regimes discussed above that fully allow the recovery of both purely economic losses and immaterial damages are the Fair Credit Reporting Act (FCRA) and the tort of public disclosure of private facts. HIPAA only does so implicitly—and only to a limited extent—by providing statutory damages in *parens patriae* actions. On the other hand, the tort of negligence is subject to the economic loss doctrine and allows the recovery of neither while the issue of recoverable damages is only addressed vaguely by the EUDPD and left entirely unresolved by COPPA, California's statutory disposal requirements, and California Assembly Bill 1950.[1360]

Lastly, it should be noted that California Senate Bill 541 entirely sidesteps the issue of recoverable damages since it does not provide for a private right of action but rather for administrative penalties to be assessed in the event of a breach.[1361]

[1358] *Cf., e.g.,* Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1008 (N.H. 2003) (woman was killed by stalker who bought the victim's address and Social Security number from the plaintiff, an Internet-based investigation service).

[1359] Economic losses are sometimes suffered due to subsequent impersonation fraud. *See* SYNOVATE, FEDERAL TRADE COMM'N – 2006 IDENTITY THEFT SURVEY REPORT 37 (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf (noting that 41% of "identity theft" victims incurred out-of-pocket expenses). Immaterial damages are even more common because, arguably, any violation of information privacy causes immaterial damages.

[1360] *See supra* chapters 5.1.6, 5.1.5.2, and 5.1.5.3.

[1361] *See supra* chapter 5.1.5.4.

5.1.7.2. Availability of Statutory Damages

The FCRA is the only regulatory policy which provides statutory damages (in cases of willful infringement).[1362] This is very significant since it may be difficult for a plaintiff to establish any specific amount of economic losses and/or immaterial damages suffered. Furthermore, statutory damages potentially also reduce the costs of litigation by eliminating difficult questions of fact. They also introduce some degree of legal certainty with regard to the amount of damages likely to be awarded.

Statutory damages can therefore be seen as a very significant instrument for ensuring that a liability regime is effective in performing a direct risk transfer from the individuals concerned to the controllers of personal information.

In EU law, statutory damages are rather rare as they are generally seen as related to punitive damages.[1363] However, in the realm of copyright law, the EU legislator has already recognized the benefit of statutory damages: article 13(1)(b) of Parliament and Council Directive 2004/48 (hereinafter *Intellectual Property Rights Enforcement Directive*, or *IPRED*)[1364] expressly allows Member States to introduce statutory damages for copyright

[1362] *See supra* chapter 5.1.3.

[1363] Punitive and statutory damages are uncommon in most Member States. However, EU law as interpreted by the ECJ does not generally disfavor punitive damages. *See* Joined Cases C-46/93 and C-48/93, Brasserie du Pêcheur SA v. Germany, 1996 E.C.R. I-1029, § 90 (holding that "it must be possible to award specific damages, such as the exemplary damages provided for by English law, pursuant to claims or actions founded on Community law, if such damages may be awarded pursuant to similar claims or actions founded on domestic law"). *Cf.* Bernhard A. Koch, *Punitive Damages in European Law, in* PUNITIVE DAMAGES: COMMON LAW AND CIVIL LAW PERSPECTIVES 197 (Helmut Koziol & Vanessa Wilcox eds., 2009).

[1364] 2004 O.J. (L 157) 45 (EC).

infringements in particular to address situations "where it would be difficult to determine the amount of the actual prejudice suffered."[1365]

5.1.7.3. Fault-Based v. Strict Liability

Fault-based liability only attaches where the defendant has been negligent or acted with intent whereas strict liability is independent of fault.[1366]

HIPAA, FCRA, and, of course, the tort of negligence all implement a fault-based liability regime.[1367] In contrast, California Senate Bill 541 and the tort of public disclosure of private facts impose strict liability.[1368] COPPA, California's statutory disposal requirements, California Assembly Bill 1950, and the EUDPD leave the issue unresolved.[1369]

It is worth mentioning that California Senate Bill 541—the only strict liability regime that covers security breach irrespective of whether the compromised information is "widely published" due to the breach[1370]—does not impose liability for all security breaches but only

[1365] IPRED recital 26. *Cf. also Commission Proposal for a Directive of the European Parliament and of the Council on measures and procedures to ensure the enforcement of intellectual property rights*, at 23, COM (2003) 46 final (Jan. 30, 2003) (stating that the aim of statutory damages was "to provide for full compensation for the prejudice suffered, which is sometimes difficult for the right holder to determine").

[1366] *See* BLACK'S LAW DICTIONARY 998 (9th ed. 2009) (noting that strict liability is also termed "liability without fault"). Note that strict liability is sometimes erroneously equated with "Gefährdungshaftung," a type of liability under German and Austrian law. *See, e.g.* Jörg Fedtke & Ulrich Magnus, *Germany, in* UNIFICATION OF TORT LAW: STRICT LIABILITY 147, 147 (Bernhard A. Koch & Helmut Koziol, eds., 2002). However, strict liability not only covers the concept of "Gefährdungshaftung" (liability for hazardous activities) but also the concept of fault-independent liability for wrongful acts ("verschuldensunabhängige Rechtswidrigkeitshaftung"). *Cf.* VIVIENNE HARPWOOD, MODERN TORT LAW 9 (6th ed. 2005) (noting that under the theory of strict liability, the plaintiff generally only has to prove that the defendant committed the act complained of, and that the damage was the result of that act).

[1367] *See supra* chapters 5.1.1, 5.1.3, 5.1.5.4, and 5.1.5.5.

[1368] *See supra* chapters 5.1.5.5, and 5.1.5.1.

[1369] *See supra* chapters 5.1.5.2, 5.1.5.3, and 5.1.6.

[1370] *See supra* chapter 5.1.5.5 (discussing the requirement of the tort of public disclosure of private facts).

if "reasonable" safeguards were not implemented.[1371] This reduces the significance of the distinction between fault-based and strict liability since a personal information controller could, in any case, shield itself from liability by implementing the required safeguards.

5.1.7.4. Availability of Class Actions

Next to the issue of recoverable damages (and the availability of statutory damages),[1372] the availability of class actions can be considered one of the most important factors determining the effectiveness of a liability regime with regard to transferring the risk of security breaches to the personal information controller.

The damages suffered by individuals due to a breach of the security of their personal information are often rather small. However, the number of affected individuals may be substantial. In a situation as this, where the risks of litigation—as compared to the potential award—are too large for any single individual, class actions are the logical solution to ensure that the affected individuals actually have a practical means of seeking redress.[1373] This ensures that a liability regime for security breaches is enforced in practice which is the only way in which it will actually transfer risk from the individuals concerned to the personal information controllers.

[1371] *See supra* chapter 5.1.5.4.

[1372] *See supra* chapters 5.1.7.1 and 5.1.7.2.

[1373] *Cf.* TIMOTHY D. COHELAN, COHELAN ON CALIFORNIA CLASS ACTIONS § 1:7 (2010-11 ed.) (noting that the primary advantage of a class action is that it effectively and efficiently brings together small claims unlikely or impractical to litigate individually); EUROPEAN COMM'N, CONSULTATION PAPER FOR DISCUSSION ON THE FOLLOW-UP TO THE GREEN PAPER ON CONSUMER COLLECTIVE REDRESS 9 (2009), *available at* http://ec.europa.eu/consumers/redress_cons/docs/consultation_paper2009.pdf (stating that "[I]n mass claims with a very low or low value of the individual claim, consumers are […] not likely to act individually as this would not be economically efficient, either for consumers themselves or for the economy as a whole").

In U.S. federal courts, class actions are governed by Rule 23 of the Federal Rules of Civil Procedure.[1374] Rule 23 is, however, not only relevant with regard to cases that raise "federal questions"[1375]: The Class Action Fairness Act of 2005[1376] gave federal district courts original jurisdiction over a broad scope of international and inter-state class actions in which the matter in controversy exceeds $5,000,000.[1377]

Under Rule 23, four prerequisites must be fulfilled before there is a possibility of a class action: (1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class.[1378] Additionally, a class action has to fit into one of three categories:

First, under Rule 23(b)(1), a class action may be certified if prosecuting separate actions would create a risk of either (1) inconsistent decisions that would establish incompatible standards of conduct for the party opposing the class or (2) impairing the interests of members

[1374] The Federal Rules of Civil Procedure are promulgated by the United States Supreme Court pursuant to the Rules Enabling Act, Pub. L. No. 73-415, 48 Stat. 1064 (1934) (codified as amended at 28 U.S.C. § 2071 et seq.). Any rule "creating, abolishing, or modifying an evidentiary privilege" has no force or effect unless approved by Act of Congress. 28 U.S.C. § 2072 (2010).

[1375] *See* 28 U.S.C. § 1331 (2010) (stating that "[federal] district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States").

[1376] Class Action Fairness Act of 2005, Pub. L. No. 109-2, 119 Stat. 4 (2005) (codified at 28 U.S.C. §§ 1332(d), 1453, and 1711-1715).

[1377] *See* 28 U.S.C. § 1332(d)(2) (stating that "[federal] district courts shall have original jurisdiction of any civil action in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and is a class action in which (A) any member of a class of plaintiffs is a citizen of a State different from any defendant; (B) any member of a class of plaintiffs is a foreign state or a citizen or subject of a foreign state and any defendant is a citizen of a State; or (C) any member of a class of plaintiffs is a citizen of a State and any defendant is a foreign state or a citizen or subject of a foreign state").

[1378] *See* FED. R. CIV. P. 23(a)(1)-(4).

of the class who are not a party to the individual actions[1379] (e.g. if individual plaintiffs face the risk of not being able to recover damages due to the defendant's limited financial resources). All members of a 23(b)(1) class are necessarily bound by the disposition as they cannot "opt out."[1380]

Second, under Rule 23(b)(2), a class action may be certified if the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole. Accordingly, this type of class action is of little relevance for mass tort claims after a security breach.

Third, under Rule 23(b)(3), a class action may be certified if (1) the questions of law or fact common to class members predominate over any questions affecting only individual members and (2) a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.[1381] While these requirements are generally easier to fulfill than those under Rule 23(b)(1), Rule 23(b)(3) has the disadvantage for plaintiffs that they have to individually notify, at their own cost, all members of the class who can be identified through reasonable effort.[1382] A notification has to inform the members of the class in particular that

[1379] *See* FED. R. CIV. P. 23(b)(1).

[1380] *See* FED. R. CIV. P. 23(c)(3)(A).

[1381] *See* FED. R. CIV. P. 23(b)(3). Four factors have to be considered: "(A) the class members' interests in individually controlling the prosecution or defense of separate actions; (B) the extent and nature of any litigation concerning the controversy already begun by or against class members; (C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and (D) the likely difficulties in managing a class action." *Id.*

[1382] *See* FED. R. CIV. P. 23(c)(2)(B). The plaintiffs have to use the best notification method "that is practicable under the circumstances." *Id. See also* Eisen v. Carlisle & Jacquelin, 417 U.S. 156, 176 1974) (holding that individual notice to identifiable class members is an unambiguous requirement of Rule 23, irrespective of whether the cost of sending individual notices would be prohibitively high to the petitioner).

they may request to be excluded from the class (i.e. "opt out") and that the judgment will be binding for them unless they opt out.[1383]

In conclusion, class actions under Rule 23(b)(1) or (b)(3) are an efficient means to claim damages pursuant to the FCRA but also pursuant to any of the liability regimes established under California or New York state law. This possibility significantly increases the effectiveness of the U.S. liability regimes with regard to the transfer of risk to personal information controllers—at least as far as data breaches are concerned that cause damages in excess of $5,000,000 or are actionable under the FCRA. For all other data breaches, the availability of class actions under California and New York state law is of great practical importance.

In California courts, § 382 of the California Code of Civil Procedure serves as the general basis for class actions. Alternatively, a class action may be brought under California's Consumers Legal Remedies Act[1384] which will be discussed subsequently.

In its relevant part, § 382 of the California Code of Civil Procedure states that "when the question is one of a common or general interest, of many persons, or when the parties are numerous, and it is impracticable to bring them all before the court, one or more may sue or defend for the benefit of all."[1385] Since this provision has not been updated since its enactment in 1872, the procedural prerequisites in California class actions are largely defined by case law[1386] which establishes three major prerequisites:

[1383] *See* FED. R. CIV. P. 23(c)(2)(B)(v), (vii).

[1384] CAL. CIV. CODE §§ 1750-84 (West 2010).

[1385] CAL. CIV. PROC. CODE § 382 (West 2010).

[1386] *See* TIMOTHY D. COHELAN, COHELAN ON CALIFORNIA CLASS ACTIONS § 2:1 (2010-11 ed.).

First, a class has to "ascertainable"[1387] which requires an objective definition of the members of the class so that each member may be located with reasonable efficiency.[1388] Ascertainability is determined by examining (1) the class definition, (2) the size of the class, and (3) the means available for identifying class members.[1389]

Second, there has to be a well-defined community of interest among the members of that class in questions of law and fact.[1390] Factors to be considered in this regard are (1) whether common questions of law or fact dominate, (2) whether the claims of the class representative are typical of the class, and (3) whether the class representative can adequately represent the class in its entirety.[1391]

Third, a substantial benefit must result both to the litigants and to the court.[1392] Consequently the certification of a class may be denied if the benefits of a class action do not exceed its costs.[1393]

[1387] *See* Richmond v. Dart Indus., Inc., 629 P.2d 23, 28 (Cal. 1981) (holding that a party seeking certification as class representative must establish existence of ascertainable class and well-defined community of interests among class members).

[1388] *See* TIMOTHY D. COHELAN, COHELAN ON CALIFORNIA CLASS ACTIONS § 2:2 (2010-11 ed.).

[1389] *See* Reyes v. San Diego County Bd. of Supervisors, 242 Cal. Rptr. 339, 343 (Cal. Ct. App. 1987) (quoting Vasquez v. Superior Court, 484 P.2d 964 (Cal. 1971)). For a discussion of these factors see for example William R. Shafton, *Complex Litigation in California and Beyond: California's Uncommon Common Law Class Action Litigation*, 41 LOY. L.A. L. REV. 783, 790 (2008).

[1390] *See* Richmond v. Dart Indus., Inc., 629 P.2d 23, 28 (Cal. 1981) (holding that a party seeking certification as class representative must establish existence of ascertainable class and well-defined community of interests among class members).

[1391] *See* Reyes v. San Diego County Bd. of Supervisors, 242 Cal. Rptr. 339, 347 (Cal. Ct. App. 1987). The third factor in particular requires that the class representative has the ability and willingness to pursue the class members' claims vigorously. TIMOTHY D. COHELAN, COHELAN ON CALIFORNIA CLASS ACTIONS § 2:4 (2010-11 ed.). *Cf.* Seastrom v. Neways, Inc., 57 Cal. Rptr. 3d 903, 907 (Cal. Ct. App. 2007) (holding that named representatives will not fairly and adequately protect the interests of the class when there are conflicts of interest between them and the class they seek to represent).

[1392] *See* Blue Chip Stamps v. Superior Court, 556 P.2d 755, 758 (Cal. 1976).

Where case law is silent, California courts apply Rule 23 of the Federal Rules of Civil Procedure.[1394] Accordingly, since § 382 of the California Code of Civil Procedure neither provides any class action types nor addresses the issues of notice requirements and "opt out," California courts adopted the federal approach outlined in Rule 23(b)[1395] and generally require notices for 23(b)(3) class actions.[1396] However, a court may impose the costs of notification on either party.[1397] This constitutes a very significant advantage for plaintiffs, thereby adding to the effectiveness of the California state law liability regimes.

In California courts, an alternative statutory basis for class actions is provided by the Consumers Legal Remedies Act (*hereinafter* CLRA).[1398] The CLRA's prerequisites are virtually identical to the prerequisites found in Rule 23(a).[1399] However, the CLRA only provides a class action for "consumers"[1400] who can claim to have suffered damages as a

[1393] *See* Kaye v. Mount La Jolla Homeowners Assn., 252 Cal. Rptr. 67, 79 (Cal. Ct. App. 1988) (citing Blue Chip Stamps v. Superior Court, 556 P.2d 755, 758 (Cal. 1976)).

[1394] *See* Vasquez v. Super. Ct., 484 P.2d 964, 977 (Cal. 1971) ("In the event of a hiatus, rule 23 of the Federal Rules of Civil Procedure prescribes procedural devices which a trial court may find useful.").

[1395] *See* Frazier v. City of Richmond, 228 Cal. Rptr. 376, 381 (Cal. Ct. App. 1986) (holding that "it is well established that in the absence of relevant state precedents, trial courts are urged to follow the procedures prescribed in Rule 23 […] for conducting class actions").

[1396] *See, e.g.,* Home Sav. & Loan Assn. v. Superior Court, 117 Cal. Rptr. 485 (Cal. Ct. App. 1974). The manner and content of a notice are described in CAL. RULES OF COURT, Rule 3.766.

[1397] *See* Civil Serv. Employees Ins. Co. v. Superior Court, 584 P.2d 497, 506 (Cal. 1978) ("California trial courts clearly possess general authority to impose notice costs on either party, plaintiff or defendant, in a class action").

[1398] CAL. CIV. CODE §§ 1750-84 (West 2010).

[1399] CAL. CIV. CODE § 1781(b) provides that a court has to permit a class action if (1) it is impracticable to bring all of the class members before the court; (2) common questions of law or fact predominate; (3) the representative plaintiff's claims are typical of the class; and (4) the representative plaintiffs will fairly and adequately protect the interests of the class. *Cf.* William R. Shafton, *Complex Litigation in California and Beyond: California's Uncommon Common Law Class Action Litigation*, 41 LOY. L.A. L. REV. 783, 824 (2008). This means that CLRA claimants neither have to prove that the class action is a superior method of adjudication, as required under § 382, nor that there is a substantial benefit to the public.

[1400] *See* CAL. CIV. CODE § 1761(d) (defining "consumer" as "an individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes").

result of any of the narrowly worded 24 unfair business practices enumerated by the CLRA.[1401] Since the causation of damages pursuant to any of the California state law liability regimes discussed above does not constitute such an unfair business practice, the CLRA is not relevant with regard to these liability regimes.[1402]

In New York courts, class actions are governed by article 9 (§§ 901 et seq.) of the New York Civil Practice Law and Rules (*hereinafter* CPLR). CPLR § 901(a) defines the following five prerequisites for any class action: (1) "numerosity"; (2) predominance of common questions of law or fact; (3) typicality of the class representative's claim; (4) adequate representation by the class representative; and (5) superiority of the class action mode of adjudication.[1403]

CPLR differs significantly from Rule 23 insofar as it does not provide a classification scheme similar to Rule 23(b).[1404] In the interest of "structural consistency and greater simplicity,"[1405] CPLR § 901(a) incorporates the "predominance of common questions" and "superiority"

[1401] CAL. CIV. CODE § 1770 (providing a list 24 proscribed practices). *See* Cal. Civ. Code § 1780(a) (stating that "[a]ny consumer who suffers any damage as a result of the use or employment by any person of a method, act, or practice declared to be unlawful by Section 1770 may bring an action against that person"). *See* CAL. CIV. CODE § 1781(a) (stating that "[a]ny consumer entitled to bring an action under Section 1780 may, if the unlawful method, act, or practice has caused damage to other consumers similarly situated, bring an action on behalf of himself and such other consumers to recover damages or obtain other relief as provided for in Section 1780").

[1402] A CLRA class action may only be possible to claim damages after a data breach if the plaintiffs can prove that the defendant claimed to have implemented certain statutorily mandated safeguards but actually failed to do so, thereby making a false representation regarding the quality of services offered. *See* CAL. CIV. CODE § 1770(7) (establishing the following prohibition: "Representing that […] services are of a particular standard, quality, or grade […] if they are of another.").

[1403] *See* CPLR § 901(a)(1)-(5).

[1404] Rule 23(b)'s classification scheme was thought to be unnecessarily complex and redundant. *See* Adolf Homburger, *State Class Actions and the Federal Rule*, 71 COLUM. L. REV. 609, 634 (1971) (raising the question with regard to 23(b)(1) and 23(b)(2) "why formulations so complex are needed to describe situations so obviously appropriate for unitary adjudication").

[1405] Adolf Homburger, *State Class Actions and the Federal Rule*, 71 COLUM. L. REV. 609, 654 (1971).

requirements found in Rule 23(b)(3),[1406] making them universally applicable to all class actions.[1407]

In all class actions brought not primarily for injunctive or declaratory relief (i.e. in particular in cases brought for money damages), "reasonable notice" has to be given to the members of the class.[1408] However, in contrast to Rule 23, individual notification of all member of the class is not necessarily required; the method of notice is rather in the court's discretion,[1409] whereas the costs of notification may be imposed on either party.[1410] "When appropriate," courts "may" give members of a class the opportunity to "opt out."[1411]

In practice, the "most troublesome" prerequisite for class actions under CPLR § 901(a) is the requirement of "predominance of common questions."[1412] In particular mass tort actions

[1406] FED. R. CIV. P. 23(a)(2) only requires that "there are questions of law or fact common to the class" while FED. R. CIV. P. 23(b)(3) additionally requires that (1) the questions of law or fact common to class members "predominate over any questions affecting only individual members", and (2) that a class action is "superior to other available methods for fairly and efficiently adjudicating the controversy."

[1407] Adolf Homburger, *State Class Actions and the Federal Rule*, 71 COLUM. L. REV. 609, 636 (1971) ("Without a predominant common core, class actions would splinter into piecemeal litigation of individual claims, unsuitable for unitary disposition. Likewise, class actions should always yield to superior devices and techniques that conform to more traditional notions of due process.").

[1408] *See* CPLR § 904(b). In actions brought primarily for injunctive or declaratory relief, notice is only required if "the court finds that notice is necessary to protect the interests of the represented parties and that the cost of notice will not prevent the action from going forward." CPLR § 904(a).

[1409] *See* CPLR § 904(c) (stating that in determining the method of notice, the court shall consider (1) the cost of giving notice by each method considered; (2) the resources of the parties and; (3) the stake of each represented member of the class, and the likelihood that significant numbers of represented members would desire to exclude themselves from the class or to appear individually).

[1410] *See* CPLR § 904(d)(I).

[1411] *See* CPLR § 903 ("When appropriate the court may limit the class to those members who do not request exclusion from the class within a specified time after notice."). However, the constitutional requirement of due process makes an opt-out right mandatory in certain cases. *Cf., e.g.,* In re Colt Industries Shareholder Litigation, 566 N.E.2d 1160, 1168 (N.Y. 1991) (holding that once parties in shareholders' suit presented court with settlement that resolved equitable issues and in turn required class members to give up all claims in damages, trial court could not approve settlement without affording Missouri corporation chance to opt out of class).

[1412] *See* Friar v. Vanguard Holding Corp., 434 N.Y.S.2d 698, 706 (N.Y. App. Div. 1980) (stating that "[t]he predominance requirement […] unquestionably is the most troublesome one in [CPLR § 901]").

based on a multitude of damaging events (e.g. in the case of defective products) have often failed to meet this requirement.[1413] However, if the members of a class suffered damages due to a single event, the "predominance" requirement is typically met. A class action for damages caused by a single security breach is therefore likely to be, at least partially, certified.[1414]

In summary, class actions available under Rule 23 of the Federal Rules of Civil Procedure as well as under California and New York state law allow mass litigations for all of the federal and state law liability regimes discussed above.

In stark contrast to the legal situation in the U.S., EU law currently does not provide for any class actions.[1415] However, the European Commission acknowledges that there are barriers which *de facto* currently impede EU consumers from obtaining effective redress.[1416] In a Green Paper adopted in 2007, the European Commission therefore initiated a policy discussion about whether to introduce some form of consumer collective redress at the EU

[1413] *See* Rosenfeld v. A. H. Robins Co., Inc., 407 N.Y.S.2d 196, 199 (N.Y. App. Div. 1978) (holding that the predominance requirement was not met for design defect claims because the question of proximate cause would vary among the members of the class); Evans v. City of Johnstown, 470 N.Y.S.2d 451, 452 (N.Y. App. Div. 1983) (main issues of whether a specific injury to property or person was caused by the sewerage plant and of the extent of any damages require individualized investigation); Geiger v. Am. Tobacco Co., 716 N.Y.S.2d 108, 109 (N.Y. App. Div. 2000) (denying certification of class of cigarette smokers who allegedly developed cancer because individual issues of addiction and use of particular product would predominate); Hurtado v. Purdue Pharma Co., 800 N.Y.S.2d 347 (N.Y. Sup. Ct. 2005) (denying certification in action by users of pain medication alleging personal injuries attributable to addiction because of predominance of individual issues such as reasons for treatment, dosages, whether other medications were being taken, past history with narcotics abuse, or specific injury sustained).

[1414] Under the CPLR, it is possible to certify a class while leaving issues not common to the class (e.g. the question of damages if statutory damages are not available) for individual determination. *See* Rosenfeld v. A. H. Robins Co., Inc., 407 N.Y.S.2d 196, 199 (N.Y. App. Div. 1978) (stating in a dictum: "where the liability issue could be isolated and treated on a class-wide basis (e.g., a typical common disaster or mass tort case), there would be strong reasons for certifying the proposed class, although the question of damage would necessarily have to be left for individual determination").

[1415] As of 2008, 13 Member States have implemented some means of consumer collective redress. *See Commission Green Paper on Consumer Collective Redress*, at 4, COM (2008) 794 final (Nov. 27, 2008).

[1416] *Id.*

level.[1417] A consultation opened by the Commission in 2009,[1418] clearly demonstrated that consumer organizations and industry representatives have strongly opposing views on the issue.[1419] It remains to be seen whether the European Commission will propose, and the European Parliament and the Council will adopt any legal instrument that provides means of consumer collective redress.

5.1.7.5. Availability of Collective Redress by Public Enforcement: *Parens Patriae* Actions

In U.S. law, the common law doctrine of *parens patriae*[1420] allows a state to sue on behalf of its citizens when its sovereign or quasi-sovereign interests are implicated and it is not merely litigating the personal claims of its citizens.[1421] Statutory *parens patriae* authority is granted to the states by numerous federal laws to circumvent the legal limits of the common law *parens patriae* doctrine.[1422]

[1417] *Id.* The introduction of means of collective redress also seems to gain popularity in other EU policy areas. *Cf. Commission White Paper on Damages actions for breach of the EC antitrust rules,* at 4, COM (2008) 165 final (Apr. 2, 2008) (stating that "[w]ith respect to collective redress, the Commission considers that there is a clear need for mechanisms allowing aggregation of the individual claims of victims of antitrust infringements").

[1418] EUROPEAN COMM'N, CONSULTATION PAPER FOR DISCUSSION ON THE FOLLOW-UP TO THE GREEN PAPER ON CONSUMER COLLECTIVE REDRESS (2009), *available at* http://ec.europa.eu/consumers/redress_cons/docs/consultation_paper2009.pdf.

[1419] EUROPEAN COMM'N, FEEDBACK STATEMENT SUMMARISING THE RESULTS OF THE WRITTEN REPLIES TO THE CONSULTATION PAPER 5 (2009), *available at* http://ec.europa.eu/consumers/redress_cons/docs/overview_results_coll_redress_en.pdf.

[1420] Literally translated, "parent of his or her country." BLACK'S LAW DICTIONARY 1221 (9th ed. 2009).

[1421] *See* Romualdo P. Eclavea, *State's standing to sue on behalf of its citizens*, 42 A.L.R. FED. 23, § 2[a] (1979). *Cf.* JAY L. HIMES, OFFICE OF THE NEW YORK ATTORNEY GENERAL, STATE PARENS PATRIAE AUTHORITY: THE EVOLUTION OF THE STATE ATTORNEY GENERAL'S AUTHORITY (2004), *available at* http://www.abanet.org/antitrust/at-committees/at-state/pdf/publications/other-pubs/parens.pdf (discussing the historical roots and the evolution of the *parens patriae* doctrine, in particular in the State of New York).

[1422] State of Cal. v. Frito-Lay, Inc., 474 F.2d 774 (9th Cir. 1973) (holding that the State, as *parens patriae*, could not bring a suit for federal antitrust law violations and recover treble damages on behalf of its citizen-consumers for injuries suffered by them). To overturn this holding, Congress passed Title III of the Hart–Scott–Rodino Antitrust Improvements Act of 1976, Pub. L. No. 94-435, 90 Stat. 1383 (1976), providing a statutory basis for

FCRA, HIPPA, and COPPA provide a statutory basis for *parens patriae* actions by the states to recover damages on behalf of the residents of a state. However, none of these federal laws address the issue of how damages, if awarded to a state, are to be distributed to the aggrieved individuals. Accordingly, this is a matter left to state law.[1423]

Parens patriae actions are a form of collective redress since they allow the claims of many aggrieved individuals to be adjudicated collectively. In contrast to class actions, they rely on the state to act on behalf of its residents. This has the advantage that State attorneys general may be willing and able to bring suit in cases where aggrieved individuals might not have sufficient incentives to bring a class action themselves. Accordingly, where *parens patriae* actions are permitted as an addition to a private cause of action, as it is the case under the FCRA, they clearly add to the effectiveness of a liability regime.

However, if *parens patriae* actions are implemented without providing a private cause of action, as it is the case for HIPAA and COPPA, the effectiveness of the liability regime is limited significantly because State attorneys general may not have sufficient resources to persecute all relevant cases.

5.1.7.6. Conclusion

The above discussion shows that there are many obstacles for a liability regime to effectively transfer information security risk to personal information controllers.

parens patriae actions by the states. *Cf.* ABA SECTION OF ANTITRUST LAW, STATE ANTITRUST PRACTICE AND STATUTES 9 (3d ed. 2004).

[1423] *Cf., e.g.,* CAL. BUS. & PROF. CODE § 16760(e) (providing that each person is to be afforded a reasonable opportunity to secure his or her appropriate portion of the monetary relief).

While the question of whether the liability regime is based on strict liability is not necessarily decisive, the recoverability of purely economic losses and/or immaterial damages can be considered a *conditio sine qua non*. Furthermore, the availability of statutory damages and a means of collective redress in the form of a class action and/or a *parens patriae* action significantly increases a liability regime's effectiveness.

Only HIPAA, FCRA, and the tort of public disclosure of private facts—which is recognized in California but not in New York—allow the recovery of purely economic losses and immaterial damages. All other liability regimes—in particular the EUDPD which does not conclusively address the issue—fail this first fundamental test, rendering them incapable of performing a meaningful risk transfer.

HIPAA, FCRA and the tort of public disclosure of private facts face other obstacles which greatly limit the effectiveness of the risk transfer: HIPAA does provide statutory damages but fails to provide a private right of action and instead exclusively relies on *parens patriae* action. Furthermore, no damages can be obtained if the failure to comply was not due to willful neglect and is corrected during a period of 30 days.[1424]

FCRA provides statutory damages, class actions, and *parens patriae* action; however, it only imposes liability if one of its regulatory requirements is violated. Since these requirements are rather narrow and specifically do not include a generally worded obligation to ensure the security of consumer information,[1425] the liability regime of the FCRA has a rather narrow scope of application, thereby only transferring a rather small portion of the risk to personal information controllers.

[1424] *See supra* chapter 5.1.1.

[1425] *See supra* chapter 5.1.3.

Lastly, the tort of public disclosure of private facts also has a very limited scope of application since it requires that the personal information be widely published and not confined to a few persons or limited circumstances.[1426]

Administrative penalties to be assessed in the event of a breach constitute an alternative form of liability. California Senate Bill 541 implements such a regime and, in doing so, has to exclusively rely on public enforcement which significantly limits the effectiveness of the risk transfer.

In summary, the liability of personal information controllers for security breaches is very limited under U.S. as well as EU law. Therefore the law as it stands today does not perform a sufficiently significant risk transfer that would address the fundamental challenge of the misalignment between risk and risk mitigation capability as applied to personal information controllers.[1427]

5.2. Liability of Service Providers

Communications service providers and online service providers transmit, store, and process evermore personal as well as other information, making the security of their services increasingly relevant for information security in general. Furthermore, by transmitting malicious third-party content, communications service providers and, to some extent, online service providers have always served as important intermediaries for all Internet-based threats, in particular for those related to malware.

[1426] *See supra* chapter 5.1.5.5.

[1427] *Cf.* NAT'L RESEARCH COUNCIL, CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 14 (2002) (stating that policy makers should "[c]onsider legislative responses to the failure of existing incentives to cause the market to respond adequately to the security challenge. Possible options include steps that would increase the exposure of […] system operators to liability for system breaches").

The following chapters will discuss the potential liability of service providers with regard to third-party content (see *infra* chapter 5.2.1) and breaches of the security of the provided services (see *infra* chapter 5.2.2).

5.2.1. Liability for Third-Party Content

Communications service providers collectively operate the physical and logical infrastructure over which all Internet-based threats are transported.[1428] This includes malware being sent over the Internet from one computer to another in order to gain unauthorized access by exploiting a software vulnerability or by performing social engineering. Once computers are compromised, they are typically joined into a "botnet"[1429] and often subsequently used to mount information security threats against yet other computers. In that case, communications service providers again act as intermediaries.

In a similar fashion, online service providers often, too, act as intermediaries: Internet-based threats are increasingly delivered via a website rather than by directly establishing a network connection with the victims' computers. For this purpose, malicious threat agents often use hosting providers to make their malware accessible to victims.[1430]

It is often assumed that communications service providers and online service providers have the capability to detect and prevent the distribution of malicious third-party content.[1431] Given

[1428] *Cf. supra* chapter 2.3.1 (discussing the role of communications providers in the information security landscape).

[1429] *See infra* chapter 7.4.2 (describing the functionality of botnets).

[1430] *Cf., e.g.,* WEBSENSE SECURITY LABS, STATE OF INTERNET SECURITY, Q3 – Q4, 2009, at 1 (2010), *available at* https://www.websense.com/assets/reports/WSL_H2_2009.pdf (finding that 95% of user-generated posts on websites are spam or contain malicious code).

[1431] *Cf.* Doug Lichtman & Eric P. Posner, *Holding Internet Service Providers Accountable, in* THE LAW AND ECONOMICS OF CYBERSECURITY 221, 223 (Mark F. Grady & Francesco Parisi eds., 2006) ("Our argument in favor of service provider liability is primarily based on the notion that ISPs are in a good position to reduce the that providers bear only a very small amount of the risks associated with that content, it could be argued that a direct risk transfer—in the form of liability for third-party content—should be performed to better align risk and risk mitigation capability.[1432] The following chapters discuss the extent of liability providers may face under the Communications Decency Act and the E-Commerce Directive. A subsequent chapter will provide a comparative analysis and will discuss to what extent providers indeed have the capability to detect and prevent the distribution of malicious third-party content.

5.2.1.1. Limitations of Liability under the Communications Decency Act

The Communications Decency Act of 1996[1433] (hereinafter *CDA*), enacted as Title V of the Telecommunications Act of 1996,[1434] was primarily intended to regulate obscene and indecent content on the Internet and on cable television. To protect service providers from encountering liability based on their voluntary efforts to block offensive content, CDA § 502—codified at and commonly referred to as "section 230" of 47 U.S.C.—introduced an important liability exception for service providers.

In 1998, the Supreme Court, in its landmark decision of *Reno v. American Civil Liberties Union*,[1435] declared significant parts of the CDA unconstitutional for violations of the First

number and severity of bad acts online […]."); Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 386 (2005).

[1432] *Cf. supra* chapter 2.4.4 (discussing the fundamental challenge of the misalignment between risk and risk mitigation capability).

[1433] Pub. L. No. 104-104, Title V, 110 Stat. 56, 113 (1996).

[1434] Pub. L. No. 104-104, 110 Stat. 56 (1996).

[1435] Reno v. Am. Civil Liberties Union, 521 U.S. 844 (1997) (holding that the CDA's "indecent transmission" and "patently offensive display" provisions (17 U.S.C. § 223(a) and (d)) abridge "the freedom of speech" protected by the First Amendment).

Amendment.[1436] However, § 230 remained unaffected by that decision,[1437] and subsequently became "one of the most important and successful laws of cyberspace."[1438]

Section 230 states that "[n]o provider […] of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[1439] Furthermore, it contains a "good samaritan" provision that stipulates that there should be no civil liability for providers of interactive computer services on account of (1) voluntarily taking action in good faith to restrict access to or availability of material that the provider considers to be objectionable; or (2) enabling or making available the technical means to restrict access to objectionable material.[1440]

This liability exemption applies to all providers of an "interactive computer service." Section 230 defines this term as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet […]."[1441] This has been construed by the courts as not only covering Internet access providers and Internet backbone

[1436] *See id.* at 876 et seq.

[1437] Only 47 U.S.C. § 230(a) and (d) were challenged in Reno v. ACLU. *See id.* at 859.

[1438] David Lukmire, *Can the Courts Tame the Communications Decency Act?: The Reverberations of Zeran v. America Online*, 66 N.Y.U. ANN. SURV. AM. L. 371, 372 (2010) (citing Recent Case, *Federal District Court Denies § 230 Immunity to Website That Solicits Illicit Content - FTC v. Accusearch, Inc.*, 121 HARV. L. REV. 2246, 2253 (2008)). For an empirical study of 184 decisions applying § 230 between its effective date, February 8, 1996, and September 30, 2009 see David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373 (2010).

[1439] 47 U.S.C. § 230(c)(1) (2010).

[1440] 47 U.S.C. § 230(c)(2). *Cf. also id.* § 230(b)(4) (expressing Congress' intent as "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material").

[1441] 47 U.S.C. § 230(f)(2).

providers but also providers of online services such as website operators[1442] or DNS registrars.[1443]

Such interactive computer service providers thus enjoy "federal immunity to any cause of action that would make [them] liable for information originating with a third-party user of the service."[1444] True to its purpose of encouraging service providers to self-regulate the dissemination of offensive material over their services, § 230 also bars lawsuits seeking to hold service providers liable for their exercise of a publisher's traditional editorial functions such as deciding whether to publish, withdraw, postpone or alter content.[1445]

However, § 230 only provides immunity for providers with regard to information (including software)[1446] "provided by *another information content provider*."[1447] Accordingly, a provider

[1442] *See* Carafano v. Metrosplash.com. Inc., 339 F.3d 1119, 1125 (9th Cir. 2003) (holding that Matchmaker.com, a commercial website, is an interactive service provider with regard to user-generated content); Barrett v. Fonorow, 799 N.E.2d 916, 922 (Ill. App. Ct. 2003) (holding that Intelisoft Multimedia, Inc., which operated the website www.internetwks.com as an "interactive computer service" while explicitly "reject[ing] the suggestion that Intelisoft is not a 'provider or user of an interactive computer service' merely because it does not provide Internet access"); Batzel v. Smith, 333 F.3d 1018, 1030 (9th Cir. 2003) (holding that services providing access to the Internet as a whole are only a subset of the services to which the statutory immunity applies). Schneider v. Amazon.com, Inc., 31 P.3d 37, 41 (Wash. Ct. App. 2001) ("Congress intended to encourage self-regulation, and immunity is the form of that encouragement. We can discern no difference between web site operators and ISPs in the degree to which immunity will encourage editorial decisions that will reduce the volume of offensive material on the Internet."). *Cf.* Catherine R. Gellis, *The State of the Law Regarding Website Owner Liability for User Generated Content*, 66 BUS. LAW. 243, 244 (2010).

[1443] *See* Hamad v. Ctr. for the Study of Popular Culture, No. A:06-CA-00285-SS, 2006 WL 3892036 (W.D.Tex. Nov. 17, 2006) (holding that "[d]omain name registrars […] are interactive service providers, since domain names are required to enable computer access to multiple users to a computer server"); Smith v. Intercosmos Media Group, Inc., No. Civ.A. 02-1964, 2002 WL 31844907, at *3 (E.D. La. Dec. 17, 2002). *Cf. also supra* chapter 2.3.1 (discussing the role of DNS registrars in the information security landscape).

[1444] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

[1445] *See id.* at 331 (noting that by passing § 230, Congress responded to Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) where the bulletin board service Prodigy was held to the strict liability standard normally applied to original publishers of defamatory statements).

[1446] *See* Green v. Am. Online (AOL), 318 F.3d 465, 471 (3d Cir. 2003) (holding that the term "information" also covers computer programs even if they do not convey any knowledge or intelligence, but merely signal a computer to halt). *Cf. also* 2 RAYMOND T. NIMMER, INFORMATION LAW § 10:64 (2010). *But see* Doug Lichtman & Eric P. Posner, *Holding Internet Service Providers Accountable, in* THE LAW AND ECONOMICS OF CYBERSECURITY 221, 252 (Mark F. Grady & Francesco Parisi eds., 2006) (criticizing Green v. Am. Online and only qualifies for immunity if it (1) provides an interactive computer service and (2) is not "responsible […] for the creation or development"[1448] of the information at issue.[1449] In the landmark case of *Zeran v. American Online*, the 4th Circuit held that it was not material whether the provider had actual knowledge of the information in question.[1450] The vast majority of § 230 decisions have also adopted this conclusion.[1451]

arguing that "information" should only cover those communications that would otherwise be regulated under defamation and similar expressive tort theories claiming that "[a] computer program that shuts down a target computer […] can be more readily and less intrusively identified").

[1447] 47 U.S.C. § 230(c)(1).

[1448] *Cf.* 47 U.S.C. § 230(f)(3) (defining "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service"). Note that there is some degree of legal uncertainty as to what it means to be "responsible […] for the creation or development of information." *See* Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1166 (9th Cir. 2008) (holding that "[b]y requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information" and further stating that "[§ 230] does not grant immunity for inducing third parties to express illegal preferences"). Hattie Harman, *Drop-Down Lists and the Communications Decency Act: A Creation Conundrum*, 43 IND. L. REV. 143, 150 et seq. (2009) (providing an in-depth discussion of the current literature and case law on this issue).

[1449] *See* Carafano v. Metrosplash.com. Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) ("Under the statutory scheme, an "interactive computer service" qualifies for immunity so long as it does not also function as an "information content provider" for the portion of the statement or publication at issue."); Prickett v. InfoUSA, Inc., 561 F. Supp. 2d 646, 651 (E.D. Tex. 2006) (quoting Carafano v. Metrosplash.com). *Cf.* Anthony v. Yahoo Inc., 421 F. Supp. 2d 1257, 1263 (N.D. Cal. 2006) ("If […] Yahoo! manufactured false profiles, then it is an 'information content provider' itself and the CDA does not shield it from tort liability."); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 717 n.11 (Cal. Ct. App. 2002) ("It is not inconsistent for eBay to be an interactive service provider and also an information content provider; the categories are not mutually exclusive. The critical issue is whether eBay acted as an information content provider with respect to the information that appellants claim is false or misleading.").

[1450] *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 et seq. (4th Cir. 1997) (holding that § 230 eliminates publisher liability—which is based on a strict liability standard—as well as distributor liability which is based on liability upon notice (or actual knowledge): "like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech"; further noting that "Congress has indeed spoken directly to the issue by employing the legally significant term 'publisher,' which has traditionally encompassed distributors and original publishers alike").

[1451] *See* David Lukmire, *Can the Courts Tame the Communications Decency Act?: The Reverberations of Zeran v. America Online*, 66 N.Y.U. ANN. SURV. AM. L. 371, 389 (2010).

This immunity does not apply with regard to any federal criminal statute[1452] or "any law pertaining to intellectual property."[1453] This means in particular that § 230 does not provide any immunity for criminal violations of the Computer Fraud and Abuse Act[1454] (hereinafter *CFAA*). However, the CFAA only penalizes intentional or knowing *acts* but not a *failure to act*,[1455] making it very unlikely that the CFAA could be used to bring criminal charges against a provider for failure to prevent violations of the CFAA by its users.[1456]

In summary, 47 U.S.C. § 230 provides broad immunity for communications service providers and online service providers as regards third party content. It even exempts providers from liability where they had knowledge of the third party content in question—so long as they were not involved in the creation or development of the content.

5.2.1.2. Limitations of Liability under the EU E-Commerce Directive

Parliament and Council Directive 2000/31[1457] (hereinafter *E-Commerce Directive*) *inter alia* harmonizes the issue of liability of providers of "information society services." Such services

[1452] 47 U.S.C. § 230(e)(1).

[1453] 47 U.S.C. § 230(e)(2).

[1454] Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified at 18 U.S.C. § 1030 as amended). *See infra* chapter 7.1.1 (providing an analysis of the CFAA).

[1455] *Cf. id.*

[1456] Indeed, no courts have addressed the issue of a provider's criminal liability under the CFAA for failure to take actions against its users. *Cf.* People v. Gourlay, No. 278214, 2009 WL 529216, at *5 (Mich. Ct. App. Mar. 3, 2009), *appeal denied*, 772 N.W.2d 382 (Mich. 2009) (stating with regard to a Michigan criminal statute that requires an intentional action that "[a]n interactive computer service provider, by providing bandwidth, by publishing content that was generated by an information content provider's use of the service's general features and mechanisms, or by knowing of the nature of the published content, has not taken an intentional action").

[1457] 2000 O.J. (L 178) 1 (EC).

are defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."[1458]

The E-Commerce Directive provides important liability exemptions[1459] which cover civil as well as criminal liability but do not affect the possibility of injunctions.[1460] These liability exemptions are provided for three types of information society service providers: "mere conduit" providers, "caching" providers, and hosting providers[1461]:

Mere conduit providers are defined as providers which offer information society services that consist of (1) "the transmission in a communication network of information provided by a recipient of the service"; or (2) "the provision of access to a communication network."[1462]

[1458] E-Commerce Directive art. 2(a) in conjunction with art. 1(2) of Parliament and Council Directive 98/34, 1998 O.J. (L 204) 37 (EC) as amended by Parliament and Council Directive 98/48, 1998 O.J. (L 217) 18, 21 (further defining "at a distance" as meaning "that the service is provided without the parties being simultaneously present"; "by electronic means" as meaning "that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means"; and "at the individual request of a recipient of services" as meaning "that the service is provided through the transmission of data on individual request"). That the service has to be "normally provided for remuneration" does not require that the remuneration stems from a service recipient. *See* E-Commerce Directive recital 18. *Cf.* Legislative Development, *Scope of the E-Commerce Directive 2000/31/EC of June 8, 2000*, 7 COLUM. J. EUR. L. 473, 475 (2001) (noting that the Directive also covers "services provided free of charge to the recipient, e.g. funded by advertising or sponsorship revenue").

[1459] *Cf.* CLAUS KASTBERG NIELSEN ET AL., STUDY ON THE ECONOMIC IMPACT OF THE ELECTRONIC COMMERCE DIRECTIVE 16 et seq. (2007), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/ecd/%20 final%20report_070907.pdf (discussing the economic significance of the Directive's limited liability provisions in general terms).

[1460] *Cf. infra* (discussing the important roles of injunctions).

[1461] For an extensive discussion of Member State legislation and national court decisions see THIBAULT VERBIEST ET AL., STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES 32 (2007), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/ecd/%20final%20report_070907.pdf.

[1462] E-Commerce Directive art. 12(1).

This covers Internet backbone providers[1463] ("transmission *in* a communication network") as well as Internet access providers[1464] ("access *to* a communication network").[1465]

The E-Commerce Directive stipulates that a mere conduit provider should not be liable for the information transmitted if it neither (1) initiates the transmission; (2) selects the receiver of the transmission; nor (3) selects or modifies the information contained in the transmission.[1466] Internet backbone providers and Internet access providers are therefore shielded from liability even if they have actual knowledge of the information in question or its illegal nature.

A slightly narrower liability exemption exists for caching providers which are defined as providers offering an information society service that consists "of the transmission in a communication network of information provided by a recipient of the service" and further entails "the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request."[1467] To benefit from the liability exemption, a

[1463] *See supra* chapter 2.3.1 (discussing Internet backbone providers from a technical perspective).

[1464] *See id.* (discussing Internet access providers from a technical perspective).

[1465] *Cf.* Patrick Van Eecke & Barbara Ooms, *ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs*, 11 J. INTERNET L. 3, 4 (2007) (referring to backbone operators and Internet access providers); Pablo Asbo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 111, 119 (2002) (stating that "transmission *in* a communication network" (emphasis added) refers to an ISP "acting as a mere 'carrier' of data provided by third parties through its network").

[1466] E-Commerce Directive art. 12(1). Note that manipulations that are of a purely "technical nature" do not disqualify a provider from the liability exemption. E-Commerce Directive recital 43. For example, every IP data packet has a time-to-live (TTL) field that is decremented by one (i.e. modified) by every router which forwards the IP data packet to another router. *See* W. RICHARD STEVENS, TCP/IP ILLUSTRATED, VOLUME 1: THE PROTOCOLS 36 (1994).

[1467] E-Commerce Directive art. 13(1). Note that "mere conduit" providers may only perform "transient" storage and may only do so for the sole purpose of carrying out the transmission. *See* E-Commerce Directive art. 12(2). "Caching" providers, on the other hand, may also perform "temporary" storage for the purpose of making the transmission *to other recipients* more efficient. *See* E-Commerce Directive art. 13(1). *Cf. also* GRAHAM J.H. SMITH, INTERNET LAW AND REGULATION 372 (4th ed. 2007) (noting that "transient" storage would "presumably cover the storage of data in RAM as it travelled through a switch").

caching provider (1) must not modify the information;[1468] (2) has to comply with conditions on access to the information;[1469] (3) has to comply with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;[1470] (4) must not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information;[1471] and (5) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that (a) the information at the initial source has been removed; (b) access to it has been disabled at the initial source; or (c) that a court or an administrative authority has ordered the initial source to perform such a removal or disablement.[1472] It is noteworthy that, similar to a mere conduit provider, a caching provider may claim immunity under the E-Commerce Directive despite having had actual knowledge of the illegal information in question. The provisions for

[1468] E-Commerce Directive art. 13(1)(a).

[1469] *Id.* art. 13(1)(b). This means that a caching provider, in order to enjoy immunity, has to fulfill any conditions of access imposed by the source of the data. *Cf.* Pablo Asbo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce,* 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 111, 121 (2002) (naming a subscription fee or the entering of specific data as examples).

[1470] E-Commerce Directive art. 13(1)(c). The most important of these rules are specified in RFC 2616: If the response sent by a web server contains an "Expires" header field, the cached response "may not normally be returned by a cache" after the date and time specified in that field. Additionally, a Cache-Control header (which may include a "max-age" directive) must also be respected. *See* R. FIELDING ET AL., HYPERTEXT TRANSFER PROTOCOL — HTTP/1.1, RFC 2616, at 110, 126 (1999), ftp://ftp.rfc-editor.org/in-notes/rfc2616.txt. *Cf. also* MARKUS HOFMANN & LELAND BEAUMONT, CONTENT NETWORKING: ARCHITECTURE, PROTOCOLS, AND PRACTICE 59 et seq. (2005).

[1471] E-Commerce Directive art. 13(1)(d). *Cf.* Patrick Van Eecke & Barbara Ooms, *ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs*, 11 J. INTERNET L. 3, 4 (2007) (noting that "[s]uch technology concerns industry-standard hit counters"). Note that this requirement is somewhat contradictory since using a cached version of a web page—instead of the original web page—necessarily interferes with the ability of the data source to obtain usage data.

[1472] E-Commerce Directive art. 13(1)(e).

caching providers in particular limit the liability of DNS service providers as regards cached domain information (i.e. domains over which the provider has no authority).[1473]

The narrowest liability exemption is granted to hosting providers which are defined as providers offering an information society service that "consists of the storage of information provided by a recipient of the service."[1474] This does not only cover providers that host entire user websites but also all "web 2.0" services that store user-generated content[1475] (e.g. a chatroom[1476] or Google's AdWords[1477]) as well as DNS service providers as regards customer-supplied information they store about the domains over which they have authority (in particular a customer's domain name and the IP address it should resolve to).[1478]

Hosting providers do not face any liability for the information stored at the request of a recipient of the service if they (1) do not have "actual knowledge of illegal activity or

[1473] *Cf. supra* chapter 2.3.2 (describing DNS caching as well as the concept of "authority" over a domain—more precisely referred to a "zone" in this context). Note that the provisions for caching providers certainly also apply to operators of proxy servers. *Cf.* ELIZABETH D. ZWICKY ET AL., BUILDING INTERNET FIREWALLS 110 et seq. (2d ed. 2000) (describing the functionality of proxies). However, as bandwidth became less of a concern in the last decade, proxy servers have become less significant in recent years, at least as regards their caching functionality.

[1474] E-Commerce Directive art. 14(1).

[1475] *Cf.* Timothy Pinto et al., *Liability of Online Publishers for User Generated Content: A European Perspective*, COMM. LAW., Apr. 2010, at 5, 6 (arguing that all websites offering user-generated content should be regarded as host providers). A recent decision by an Italian court which held that YouTube.com was not a hosting provider in particular because it earns money from user-generated content by way of selling advertising was made in blatant disregard for the express language of the E-Commerce Directive which covers "services which are not remunerated by those who receive them." E-Commerce-Directive recital 18. *Cf.* Giovanni Sartor et al., *The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*, 18 INT'L J.L. & INFO. TECH. 356, 369 et seq. (2010). *Cf. also* Graham Smith, *Online Intermediary Liability,* CYBERSPACE LAW., Apr. 2009, at 19 (noting with regard to national court decisions in general that "[c]onsiderable uncertainty has surrounded the question of what qualifies as a host under Article 14").

[1476] *See First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, at 12 n.64, COM (2003) 702 final (Nov. 21, 2003).

[1477] *See* Joined Cases C-236/08, C-237/08, and C-238/08, Google France SARL v. Louis Vuitton Malletier SA, 2010 E.C.R. I-0000, § 110-11.

[1478] *Cf. supra* chapter 2.3.2 (describing the concept of "authority" over a domain—more precisely referred to a "zone" in this context).

information";[1479] and (2) upon obtaining such knowledge, act expeditiously to remove or to disable access to the information.[1480] As regards claims for damages, a lack of "actual knowledge of illegal activity or information" is not sufficient; a provider furthermore must "not [be] aware of facts or circumstances from which the illegal activity or information is apparent."[1481] The E-Commerce Directive thereby creates a notice-and-takedown regime for hosting providers. However, it does not prescribe any specific procedures to be followed, e.g. regarding the form and the content of a notice,[1482] and rather leaves this important issue to self-regulation.[1483]

As mentioned *supra*, none of these liability exemptions affect the possibility of injunctions or, more specifically, "affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to *terminate* or *prevent* an infringement."[1484] This possibility of injunctions creates a tension with article 15 of the

[1479] E-Commerce Directive art. 14(1)(a).

[1480] *See* E-Commerce Directive art. 14(1)(b).

[1481] E-Commerce Directive art. 14(1)(a).

[1482] *Cf.* Patrick Van Eecke & Barbara Ooms, *ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs*, 11 J. INTERNET L. 3, 5 (2007).

[1483] *See* E-Commerce Directive recital 40 (stating that "rapid and reliable procedures for removing and disabling access to illegal information […] could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States"). *Cf. First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, at 14, COM (2003) 702 final (Nov. 21, 2003) (noting that all Member States except Finland have adopted a self-regulatory approach in this regard). *Cf. also* Rosa Julià-Barceló & Kamiel J. Koelman, *Intermediary Liability in the E-Commerce Directive: So Far So Good, But It's Not Enough*, 16 COMPUTER L. & SECURITY REP. 231, 224 (2000) (arguing that "a legal regime that threatens Internet service providers with liability based upon 'constructive knowledge' obtained from private complaints [would] encourage the virtually automatic and systematic removal by intermediaries of material from the public domain," thereby "unduly threaten[ing] freedom of expression and fair competition").

[1484] E-Commerce-Directive art. 12(3), 13(2), 14(3) (emphasis added). Article 14(3) further adds, somewhat redundantly: "nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information."

E-Commerce Directive which provides that "Member States shall not impose a general obligation on providers […] to monitor the information which they transmit or store."[1485] A provider could, for example, not prevent the transmission of a certain malware without monitoring all communications to detect and subsequently block the malware.

This raises the question: When does an injunction amount to a general monitoring obligation prohibited under the Directive? In other words, what aspect of the monitoring obligation must not be of a "general" nature (i.e. has to be of a specific nature): the obligation's legal source, the nature of the information to be monitored, or the technical source (or destination) of the information to be monitored?

Indeed, if article 15 of the E-Commerce Directive only required that the legal source of the monitoring obligation be specific, injunctions would comply with article 15 as long as they are not directed at all (or most) of the providers of a Member State.[1486]

If specificity is only required with regard to the nature of the infringing information, an injunction prohibiting a mere conduit provider from transferring a particular malware (e.g. the

[1485] E-Commerce Directive art. 15(1). Note that ePrivacy Directive art. 15 allows Member States to adopt "legislative measures providing for the retention of data for a limited period" justified on the grounds that they are "necessary, appropriate and proportionate measure[s] within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system." ePrivacy Directive art. 15(1). Parliament and Council Directive 2006/24, 2006 O.J. (L 105) 54 (commonly referred to as the "Data Retention Directive") goes one step further, requiring Member states to introduce obligations for "providers of publicly available electronic communications services or of public communications networks" (these are "mere conduit" providers) "with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime." *Id.* art. 1(1). For an extensive discussion of the Data Retention Directive see Lukas Feiler, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, 1 EUR. J. OF L. & TECH. 3 (2010), http://ejlt.org//article/view/29/75. However, neither ePrivacy Directive art. 15 nor the Data Retention Directive have direct relevance for the question of when an injunction amounts to a general monitoring obligation prohibited under art. 15 of the E-Commerce Directive.

[1486] *Cf.* E-Commerce Directive recital 47 (stating that the prohibition of general monitoring obligations "does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation").

"Conficker" worm) over its network would comply with article 15. The fact that such an injunction could only be complied with by monitoring the content of the communications of all its users would be immaterial. Such "deep packet inspection" would not only be very costly for the mere conduit provider, it would also raise issues of proportionality with regard to the interference with the fundamental rights to privacy and data protection[1487] and the principle of confidentiality of communications.[1488]

If specificity is required regarding the technical source or destination of the infringing information, any monitoring obligation resulting from an injunction would be much more limited as regards the number of affected users. It would be comparatively inexpensive for mere conduit providers, caching providers, or hosting providers to perform such monitoring, particularly if the monitoring is based on IP addresses. The level of interference with the rights of users would also be drastically reduced.

An argument could therefore be made that the prohibition of "general" monitoring obligations requires specificity at least with regard to the technical source or destination of the infringing information. However, legal uncertainty remains until the ECJ addresses the issue.[1489]

[1487] Charter of Fundamental Rights of the European Union, art. 7 and 8, 2010 O.J. (C 83) 389, 393.

[1488] *See* ePrivacy Directive art. 5.

[1489] The ECJ is expected to do so in Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM) in which the Cour d'appel de Bruxelles asked the ECJ whether it would constitute a violation of, *inter alia*, the E-Commerce Directive to order a provider to introduce, "for all its customers, in abstracto and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the sharing of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent." *See* 2010 O.J. (C 113) 20.

National courts have increasingly issued injunctions, in particular against hosting providers, effectively requiring them to monitor all user-generated content.[1490]

In summary, the E-Commerce Directive provides significant limitations on the liability of mere conduit providers and caching providers while only limiting the liability of hosting providers if they are not aware of facts or circumstances from which the illegal activity or information is apparent. However, none of these liability limitations apply to injunctions which may effectively require providers to perform monitoring of all third-party content.

5.2.1.3. Comparative Assessment

The liability limitations provided by the CDA and the E-Commerce Directive exhibit substantial differences regarding (1) the question whether different types of providers should be treated differently; (2) whether to limit liability irrespective of the legal nature of the liability; and (3) whether to also cover injunctions.

Regarding the first issue, the CDA treats all types of interactive computer service providers alike and covers in particular Internet access providers, Internet backbone providers, website operators and DNS registrars. A provider may claim immunity under the CDA despite having had actual knowledge of the information in question or its illegal nature.

In stark contrast to this uniform approach, the E-Commerce Directive differentiates between mere conduit providers, caching providers, and hosting providers: only the former two are allowed to claim immunity if they had actual knowledge of the information or its illegal nature. Hosting providers, on the other hand, are subject to a notice-and-takedown regime.

[1490] Patrick Van Eecke & Barbara Ooms, *ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs*, 11 J. INTERNET L. 3, 6 et seq. (2007) (discussing numerous decisions by national courts).

Incidentally, this regime is similar to (but lacks the specific procedures provided by) the Digital Millennium Copyright Act[1491] which only applies to copyright infringement and is therefore not discussed in this context.[1492]

As regards the second issue of the liability regime's application irrespective of the legal nature of the liability, the E-Commerce Directive implements a horizontal approach, "meaning that [it covers] liability, both civil and criminal, for all types of illegal activities initiated by third parties."[1493] The CDA, on the other hand, explicitly provides that its limitations on liability do not affect federal criminal statutes and intellectual property laws.

The third issue of whether the liability limitations also cover injunctions is particularly significant since injunctions have the potential to effectively hollow out the liability limitations. The CDA does provide immunity from injunctions while the E-Commerce Directive expressly does not. The E-Commerce Directive thereby creates significant legal uncertainties in relation to its prohibition of "general" monitoring obligations.

In conclusion, the CDA provides liability limitations that are much stronger than those under the E-Commerce Directive. Not only does the CDA—in contrast to the E-Commerce Directive—bar injunctions, it also provides immunity for hosting providers even if they have had actual knowledge of infringing information.

[1491] Pub. L. No. 105-304, § 202, 112 Stat. 2860, 2877 (1998) (codified at 17 U.S.C. § 512).

[1492] For a brief comparison between the liability regime under the E-Commerce Directive and that under the Digital Millennium Copyright Act see Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 397 (2005).

[1493] *First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, at 12, COM (2003) 702 final (Nov. 21, 2003).

However, no cases have been reported in which the possibility of injunctions under the E-Commerce Directive has been used to order a provider to refrain from distributing malware or in any other way acting as an intermediary for Internet-based information security threats. This suggests that the legal differences of the liability regimes of the CDA and the E-Commerce Directive have indeed been of little practical relevance for information security.

Furthermore, the assumption that communications service providers and online service providers have the capability to detect and prevent the distribution of malicious third-party content has to be challenged.

Technically speaking, the detection of malicious content is a very difficult task. Any network-based anti-malware software that has been developed for this purpose primarily relies on pattern-matching techniques. This requires the manufacturer of the anti-malware software to develop a pattern (also referred to as a "signature" in this context) for every newly discovered malware. This does not only require vast amounts of resources;[1494] more importantly it means that anti-malware software is typically only able to detect *known* malware.[1495] However, due to the rapid growth of malware and the self-modifying nature of advanced malware,[1496] a significant amount of malware is indeed *unknown*. To address this problem, most anti-malware software additionally use some kind of heuristic detection mechanism.

[1494] *Cf.* JOHN VIEGA, THE MYTHS OF SECURITY: WHAT THE COMPUTER SECURITY INDUSTRY DOESN'T WANT YOU TO KNOW 45 (2009) (describing the scalability problems created for anti-malware software manufacturers due to "[t]housands of new pieces of malware com[ing] out every day").

[1495] *Cf.* James S. Tiller, *Access Control, in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 93, 199 (Harold F. Tipton ed., 2007) (noting that a signature-based intrusion detection system "is only as good as the latest signature database on the system"); SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 252 (4th ed. 2008) ("This type of IDS is weak against new types of attacks because it can recognize only the ones that have been previously identified and have had signatures written for them.").

[1496] *Cf.* Ed Skoudis, *Hacker Attacks and Defenses, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 965, 971 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (noting that, in the very near future, "[w]e will see polymorphic worms, which change their patterns every time they run and spread to a new system.").

Heuristic methods, however, only have limited benefits: The prior probability (or "base rate") of any given data packet on the Internet being malicious is indeed very low. If we assume, for the purpose of a demonstrative calculation, that it is even as high as 1:1,000,000, a heuristic detection mechanism that has an accuracy of 99.99% (i.e. a false positive and a false negative rate of 0.01%) would "flag" 100 non-malicious packets for each malicious packet.[1497] Such a high false positive rate would have a devastating effect on the reliability of Internet communications. In order to decrease the false positive rate, the sensitivity of the anti-malware software has to be decreased which necessarily also decreases the true positive rate (the rate at which malicious packets are identified as such). This limits the benefits of heuristic detection methods.[1498]

It therefore cannot be assumed that providers, even if they invested significant financial resources, would be able to detect most of the malicious content. Accordingly, a liability regime that generally transfers the risk associated with malicious content to intermediary providers—effectively requiring them to detect all malicious traffic—would indeed not be transferring the risk to a party fully capable of mitigating it.[1499]

[1497] Not taking into account the prior probability, or base rate, of any packet being malicious leads to the so-called "base-rate fallacy." *See* Stefan Axelsson, *The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection*, 1999 ACM CONFERENCE ON COMPUTER AND COMMC'NS SECURITY 1. *See also supra* chapter 2.4.2 (discussing and providing further references for the base rate fallacy).

[1498] *Cf.* Stefan Axelsson, *The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection*, 1999 ACM CONFERENCE ON COMPUTER AND COMMC'NS SECURITY 1, 6 (stating that, due to the base rate fallacy problem, "the factor limiting the performance of an intrusion detection system is not the ability to identify behaviour correctly as intrusive, but rather its ability to suppress false alarms").

[1499] The incorrect assumption that providers could detect all—or at least most—malicious content often serves as a basis for policy proposals that entail making providers generally liable for malicious third-party content. *See, e.g.,* Doug Lichtman & Eric P. Posner, *Holding Internet Service Providers Accountable, in* THE LAW AND ECONOMICS OF CYBERSECURITY 221, 223 (Mark F. Grady & Francesco Parisi eds., 2006) ("Our argument in favor of service provider liability is primarily based on the notion that ISPs are in a good position to reduce the number and severity of bad acts online […]."); Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 386 (2005).

However, the E-Commerce Directive might allow injunctions ordering a provider to refrain from transmitting a particular malware—which is impossible to detect if it is self-modifying[1500]—or even from transmitting any malware. Such a far-reaching obligation would indeed not serve to align risk and risk mitigation capability.

A liability regime that transfers risk only to the extent that providers have the capacity to mitigate it, would have to implement a notice-and-takedown approach that does not obligate providers to perform any monitoring for malicious content. To meet this requirement, notices would have to clearly identify the technical source of the content by using an IP address or a domain name. The E-Commerce Directive fails in this regard because its notice-and-takedown regime does not provide any detailed requirements for the form or content of a notice.

5.2.2. Liability for Security Breaches

It has to be reiterated that security breaches cover all events that impair the confidentiality, integrity, or availability of information.[1501] Accordingly, the temporary loss of information availability also has to be considered a security breach.

In particular the *availability* of Internet access services and online services are of great relevance. If an Internet access provider's services become unavailable, so will all information stored online for all its subscribers. Similarly, if an online service provider is unavailable, so is all the information stored by that provider. "Cloud computing" has led to an increased migration of desktop applications—and all information associated with them—to

[1500] *See supra*.

[1501] *Cf.* chapter 2.1 (defining information security).

online service providers, making their availability much more important for the average user.[1502]

For example, a growing number of individual users and small businesses rely on Google's or Microsoft's online services to manage their e-mails (using Gmail or Windows Live Hotmail), to maintain a personal calendar (using Google Calendar or Windows Live Hotmail Calendar), and to create, edit and store their documents (using Google Docs or Windows Live Office).

Depending on the nature of the information stored on behalf of users, breaches of confidentiality or integrity can be equally significant for users.[1503] However, they typically are in no position to mitigate the risk of a security breach. The only entity that could implement security measures to perform meaningful risk mitigation is the service provider.

It is in this context that the question arises to what extent Internet access providers and online service providers are liable to their customers for breaches of information confidentiality, integrity, or availability.

Internet access providers and online service providers typically have a contractual relationship with the users whose data they transmit or store on their behalf. This chapter will therefore only discuss regulatory measures in the area of contractual liability. For a discussion of the

[1502] In October 2009 it was reported that users of T-Mobile Sidekick, a service that had been previously acquired by Microsoft, had lost their contacts, calendar entries, to-do lists and photos due to a "server failure" (and an apparent lack of backups). *See* Daniel Ionescu, *Microsoft Red-Faced After Massive Sidekick Data Loss*, PCWORLD, Oct. 12, 2009, *available at* http://www.pcworld.com/article/173470/microsoft_redfaced_after_massive_sidekick_data_loss.html.

[1503] *Cf., e.g.,* Jason Kincaid, *Facebook Bug Reveals Private Photos, Wall Posts*, WASHINGTONPOST.COM, Mar. 20, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/03/21/AR2009032104050.html; Jason Kincaid, *Google Privacy Blunder Shares Your Docs Without Permission*, TECHCRUNCH.COM, Mar. 7, 2009, http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/; Elinor Mills, *Twitter's network gets breached again*, CNET.COM, May 1, 2009, http://news.cnet.com/8301-1009_3-10231847-83.html?tag=mncol;txt.

issues concerning non-contractual liability for breaches of the security of personal information see *supra* chapter 5.1.

For a discussion of the issues concerning contractual liability, it should be pointed out as a preliminary matter that many online services are claimed by their providers to be offered for free when indeed they are not: The terms of services commonly state that the user grants the provider the right to use any uploaded content for the purposes of personalized advertising[1504] or even the right to transmit personal information to third parties.[1505]

5.2.2.1. Liability Under U.S. Law

Internet access providers as well as online service providers typically disclaim all liabilities and warranties to the extent permissible under the applicable law.[1506] The question therefore is which limits federal law and state law impose for such disclaimers.[1507]

[1504] *See, e.g.,* http://www.google.com/accounts/TOS (last accessed Feb. 10, 2011) ("Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be *targeted to the content of information stored on the Services, queries made through the Services* or other information." (emphasis added)).

[1505] *See, e.g.,* http://www.facebook.com/#!/policy.php (last accessed Feb. 10, 2011) ("In order to provide you with useful social experiences off of Facebook, we occasionally need to provide General Information about you to pre-approved third party websites and applications that use Platform at the time you visit them (if you are still logged in to Facebook). Similarly, when one of your friends visits a pre-approved website or application, it will receive General Information about you so you and your friend can be connected on that website as well (if you also have an account with that website).").

[1506] For example, Comcast's subscriber agreement states that "the services are provided 'as is,' without warranty of any kind, either express or implied." *See* http://www.comcast.com/Corporate/Customers/Policies/Subscriber Agreement.html (last accessed Feb. 10, 2011). Similarly, Gmail's Terms of Service state that "you expressly understand and agree that your use of the services is at your sole risk and that the services are provided 'as is' and 'as available.'" *See* http://www.google.com/accounts/TOS (last accessed Feb. 10, 2011).

[1507] Further note that implied warranties are typically not recognized for services and therefore do not even have to be disclaimed. *See* Milau Associates, Inc. v. N. Ave. Dev. Corp., 391 N.Y.S.2d 628, 629-30 (N.Y. App. Div. 1977), *aff'd sub nom.*, 368 N.E.2d 1247 (N.Y. 1977) (holding that there is no implied warranty with respect to services under common law); Huntington Beach Union High v. KPI Architects, No. 04CC00121, 2004 WL 5639743 (Cal. Super. Ct. Dec. 16, 2004) (stating that an action for breach of implied warranty for services rendered is not permissible; citing Gagne v. Bertran, 275 P.2d 15 (Cal. 1954)). *Cf. also* JAMES ACRET, CONSTRUCTION LITIGATION HANDBOOK § 14:2 (2d ed. 2010).

Warranties are generally subject to the federal Magnuson-Moss Warranty Act (MMWA),[1508] article 2 of the Uniform Commercial Code (UCC),[1509] and, in California, the Song-Beverly Consumer Warranty Act.[1510]

However, MMWA's material scope of application is limited to the sale[1511] of "tangible personal property."[1512] It therefore does not apply to the provision of services, in particular Internet access services or online services.[1513]

UCC article 2 which has been adopted in California[1514] and New York,[1515] only applies to the "sale"[1516] of "goods."[1517] It therefore also does not apply to Internet access services or online

[1508] Magnuson-Moss Warranty Act, Pub. L. 93-637, 88 Stat. 2183 (1974) (codified at 15 U.S.C. §§ 2301-12).

[1509] The Uniform Commercial Code is a model law jointly developed by the National Conference of Commissioners on Uniform State Laws (NCCUSL) and the American Law Institute (ALI).

[1510] CAL. CIV. CODE § 1790 et seq. (West 2010).

[1511] *See* 15 U.S.C. § 2301(6) (2010) (defining "written warranty" as "(A) any written affirmation of fact or written promise made in connection with the *sale* of a consumer product […], or (B) any undertaking in writing in connection with the *sale* by a supplier of a consumer product to refund, repair, replace, or take other remedial action with respect to such product […]" (emphasis added)).

[1512] *See* 15 U.S.C. § 2301(1) (defining "consumer product" as "any tangible personal property which is distributed in commerce and which is normally used for personal, family, or household purposes"). *Cf.* Rebecca Crandall, Recent Development, *Do Computer Purchasers Need Lemon Aid?*, 4 N.C. J.L. & TECH. 307, 316 (2003).

[1513] *Cf.* MARY DEE PRIDGEN, CONSUMER PROTECTION AND THE LAW § 14:5 (2010).

[1514] CAL. COM. CODE § 2101 et seq. (West 2010).

[1515] N.Y. U.C.C. LAW § 2-101 et seq. (McKinney 2010).

[1516] UCC § 2-106(1); CAL. COM. CODE § 2106(1); N.Y. U.C.C. LAW § 2-106(1) (stating that "a 'sale' consists in the passing of title from the seller to the buyer for a price").

[1517] UCC § 2-105(1); CAL. COM. CODE § 2105(1); N.Y. U.C.C. LAW § 2-105(1) (defining "goods" as "all things (including specially manufactured goods) which are movable at the time of identification to the contract for sale […].").

services. Similarly, California's Song-Beverly Consumer Warranty Act also only applies to the "sale"[1518] of "consumer goods."[1519]

Accordingly, under U.S. law, Internet access providers and online service providers can successfully disclaim all warranties and can thereby avoid contractual liability for most security breaches.

5.2.2.2. Liability Under EU law

Mirroring the legal situation in the U.S., EU law also does not regulate the contractual liability of Internet access providers and online service providers. Parliament and Council Directive 1999/44[1520] (hereinafter *Consumer Sales Directive*) as well as Council Directive 85/374[1521] (hereinafter *Product Liability Directive*) only apply to "consumer goods"[1522] or "products."[1523]

[1518] CAL. CIV. CODE § 1791(n) (defining the term "sale" as either the "passing of title from the seller to the buyer for a price" or "[a] consignment for sale").

[1519] CAL. CIV. CODE § 1791(a) (defining the term "consumer goods" as "any new product or part thereof that is used, bought, or leased for use primarily for personal, family, or household purposes […]").

[1520] 1999 O.J. (L 171) 12 (EC). *Cf. infra* chapter 5.3.4 (discussing the Consumer Sales Directive in the context of software manufacturer liability).

[1521] 1985 O.J. (L 210) 29 (EEC) as amended by Parliament and Council Directive 1999/34, 1999 O.J. (L 141) 20 (EC). *Cf. infra* chapter 5.3.3 (discussing the Product Liability Directive in the context of software manufacturer liability).

[1522] *See* Consumer Sales Directive art. 1(2)(b) (defining "consumer goods" as "any tangible movable item […]").

[1523] *See* Product Liability Directive art. 2 (defining "products" as "all movables even if incorporated into another movable or into an immovable [including] electricity").

The Commission has previously proposed the adoption of a directive on the liability of suppliers of services.[1524] That proposal was, however, ultimately withdrawn[1525] due to opposition from the Council.[1526]

Lastly, it should be pointed out that EU law does impose liability on one particular type of service providers: certification-service-providers.[1527] Pursuant to article 6 of the eSignature Directive, a certification-service-provider—unless it can prove that it did not act negligently—is liable for damage caused to any third party (including the signatory itself) who reasonably relied on a provider-issued qualified certificate (1) being accurate at the time of issuance (e.g. contains a valid name or, if identified as such, a pseudonym);[1528] (2) containing all the details prescribed for a qualified certificate;[1529] (3) containing (or identifying) a public key which corresponds to a private key that, at the time of the issuance of the certificate, was held by the signatory identified in the certificate (this requires providers to authenticate signatories before issuing them certificates);[1530] and (4) being subject to

[1524] *See Commission Proposal for a Council Directive on the liability of suppliers of services*, COM (1990) 482 final (Dec. 20, 1990).

[1525] *Commission Communication on new directions on the liability of suppliers of services*, COM (1994) 260 final (June 23, 1994).

[1526] *Cf.* HANS-W. MICKLITZ, REGULATORY STRATEGIES ON SERVICES CONTRACTS IN EC LAW, EUI WORKING PAPER LAW NO. 2008/06, at 9 (2008), *available at* http://ssrn.com/abstract=1093643. *Cf. also* http://ec.europa.eu/consumers/cons_safe/serv_safe/liability/index_en.htm (last accessed Feb. 10, 2011).

[1527] *Cf. supra* chapter 4.3.3 (discussing the meaning of the term "certification-service-provider").

[1528] *See* eSignature Directive art. 6(1)(a). This relates to the provider's function as a Registration Authority. *Cf.* CARLISLE ADAMS & STEVE LLOYD, UNDERSTANDING PKI: CONCEPTS, STANDARDS, AND DEPLOYMENT CONSIDERATIONS 86 (2d ed. 2003) (describing the role of a Registration Authority).

[1529] *See* eSignature Directive art. 6(1)(a). The mandatory contents of a qualified certificate are set out in eSignature Directive annex I.

[1530] *See* eSignature Directive art. 6(1)(b). For example, in January 2001 the U.S.-based Certification Authority VeriSign, Inc. issued two certificates for "Microsoft Corporation" to someone posing as a Microsoft employee. *See* Robert Lemos, *Microsoft warns of hijacked certificates*, CNET.COM, Mar. 22, 2001, http://news.cnet.com/2100-1001-254586.html&tag=tp_pr. *Cf. also* Carl Ellison & Bruce Schneier, *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure*, 16 COMPUTER SECURITY J. 1, 4-5 (2000), *available at* immediate revocation should the private key become compromised.[1531] In summary, liability attaches if the provides fails to properly authenticate signatories, issue certificates securely, or revoke certificates immediately.

Remarkably, article 6 of the eSignature Directive does not clearly answer the question of whether providers would be liable if *their* private key is compromised. Anyone who obtained a certification-service-provider's private key (the "root" private key) could issue arbitrary certificates in its name, destroying the entire hierarchy of trust.[1532] Article 6 only imposes liability with regard to qualified certificates "issued" by the certification-service-provider. No case law exists on this issue but it seems unlikely that this provision would cover certificates being issued in the provider's name but by a malicious third party.

5.2.2.3. Comparative Assessment

Neither U.S. law nor EU law impose limitations on warranty disclaimers by Internet access providers or online service providers. This allows them to largely avoid contractual liability for security breaches, leading to a misalignment between risk and risk mitigation capability:

In particular where users experience high switching costs, providers do not have high incentives to invest more in the security of their services since it is unlikely that a single security breach would offset these switching costs. Such switching costs are typically either

http://www.schneier.com/paper-pki.pdf (discussing the challenge of authenticating individuals or corporations before issuing certificates to them).

[1531] *See* eSignature Directive art. 6(2). An additional less security-relevant cause of liability is established by eSignature Directive art. 6(1)(c): a third party must have relied on a provider-issued certificate "for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both."

[1532] *Cf.* Geoffrey C. Grabow, *Preserving Public Key Hierarchy, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1175, 1177 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) ("If one cannot determine which CAs are to be trusted, then there is no way to determine which users' certificates are to be trusted. This causes the complete collapse of the entire hierarchy, from the top down.").

created by contractual means (e.g. a contractual penalty for early cancellation) or technological means (e.g. the difficulty of data portability).[1533] Internet access providers and online service providers therefore only bear a small portion of the risk associated with security breaches. They are, nonetheless, the only entities capable of mitigating the risk of a security breach.

That a better alignment of risk and risk mitigation capability can be rather easily accomplished is demonstrated by the eSignature Directive which introduces a fault-based liability regime for certification-service-providers. This liability regime transfers the risks associated with signatory authentication, certificate issuance, and certificate revocation to the only entity capable of mitigating them: certification-service-providers.

As regards Internet access providers and online service providers, policy makers in the U.S. as well as in the EU would be well advised to address the misalignment between risk and risk mitigation capability by limiting the extent to which Internet access providers and online service providers can disclaim warranties for services that are offered in exchange for money or the assignment of rights to uploaded data. Corresponding policy proposals are presented *infra* in chapters 9.3.2 and 9.4.2.

5.3. Liability of Software Manufacturers

Under this policy, manufacturers, which may or may not have a contract with the aggrieved party, can be held liable for damages caused by a defect in their software products. The

[1533] *Cf. A comprehensive approach on personal data protection in the European Union*, at 8, COM (2010) 609 final (Nov. 4, 2010) (stating that the Commission will examine ways to ensure data portability "i.e., providing the explicit right for an individual to withdraw his/her own data (e.g., his/her photos or a list of friends) from an application or service so that the withdrawn data can be transferred into another application or service, as far as technically feasible, without hindrance from the data controllers").

following chapters will analyze the extent to which software manufacturers can be held liable under U.S. and EU law, in particular for security vulnerabilities.

5.3.1. Product Liability Under U.S. Law

Product liability can be defined as "a manufacturer's or seller's tort liability for any damages or injuries suffered by a buyer, user, or bystander as a result of a defective product."[1534] It is primarily a matter of state law and can be based on a theory of strict liability or negligence.[1535]

5.3.1.1. Strict Tort Liability

Under the theory of strict liability, which can generally not be avoided by contractual means,[1536] it is immaterial whether the defendant acted with due care.[1537]

Under California law, "[a] manufacturer is strictly liable in tort when an article he places on the market, knowing that it is to be used without inspection for defects, proves to have a defect that causes injury to a human being."[1538] This equally applies to all other participants in the chain of distribution[1539] which are jointly and severally liable.[1540]

[1534] BLACK'S LAW DICTIONARY 1328 (9th ed. 2009).

[1535] *Cf.* Merrill v. Navegar, Inc., 28 P.3d 116, 124 (Cal. 2001) (stating that a plaintiff may seek recovery in a products liability case either on the theory of strict liability in tort or on the theory of negligence).

[1536] Westlye v. Look Sports, Inc., 22 Cal. Rptr. 2d 781, 799 (Cal. Ct. App. 1993) (holding that it would violate public policy to honor disclaimers in products cases based on strict liability). Velez v. Craine & Clark Lumber Corp., 305 N.E.2d 750, 754 (N.Y. 1973). *Cf.* RICHARD J. HEAFEY & DON M. KENNEDY, PRODUCT LIABILITY: WINNING STRATEGIES AND TECHNIQUES § 2.01 (2006).

[1537] *See* Greenman v. Yuba Power Products, Inc., 377 P.2d 897, 900 (Cal. 1963); Codling v. Paglia, 32 N.Y.2d 330, 342 (N.Y. 1973).

[1538] Greenman v. Yuba Power Prods., Inc., 377 P.2d 897, 900 (Cal. 1963).

[1539] Vandermark v. Ford Motor Co., 391 P.2d 168 (Cal. 1964); Godoy v. Abamaster of Miami, Inc., 754 N.Y.S.2d 301, 304 (N.Y. App. Div. 2003). *Cf.* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 1

Under New York law, in order to prove a *prima facie* case, a plaintiff has to prove the following elements: (1) the defendant manufactured for sale, or sold, distributed, leased, or otherwise marketed an item; (2) the item constituted a "product"; (3) the product was "defective"; (4) the plaintiff sustained an injury; and (5) the defect was a substantial factor in causing the injury.[1541]

With regard to software, the following elements make it very difficult to establish a *prima facie* case under both California and New York law: (1) the term "product"; (2) defect; (3) proximate cause; and (4) recoverable damages.

Restatement (Third) defines the term "product" as "tangible personal property distributed commercially for use or consumption."[1542] It further states that other items, "such as […] electricity, are products when the context of their distribution and use is sufficiently analogous."[1543] However, services are not products, even when provided commercially.[1544]

Commentators have argued that commercial off-the-shelf software (COTS) should not be considered a service because, unlike traditional services (e.g. hair-cuts or legal services), it is

(1998) (stating that "[o]ne engaged in the business of selling or otherwise distributing products who sells or distributes a defective product is subject to liability for harm to persons or property caused by the defect").

[1540] Bostick v. Flex Equip. Co., Inc., 54 Cal.Rptr.3d 28, 34 (Cal. Ct. App. 2007) (holding that Proposition 51 which made liability for noneconomic damages several only rather than joint and several—*see* CAL. CIV. CODE §§ 1431.1-5—does not apply in a strict products liability action involving a single indivisible injury).

[1541] *See* Caprara v. Chrysler Corp., 52 N.Y.2d 114, 123 (N.Y. 1981). *Cf. also* LEE S. KREINDLER ET AL., 15 NEW YORK LAW OF TORTS § 16:18 (2010).

[1542] RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 19 (1998).

[1543] *Id.*

[1544] *Id. See* Shepard v. Alexian Brothers Hosp., 109 Cal.Rptr. 132, 136 (Cal. Ct. App 1973) (holding that blood transfusion must be regarded as service, rendering doctrine of strict liability in tort inapplicable); Goldfarb v. Teitelbaum, 540 N.Y.S.2d 263, 263 (N.Y. App. Div. 1989) (holding that dentist's placement of prosthesis in patient's mouth as part of procedure to cap her teeth did not constitute "sale" of device as required for causes of action sounding in products liability).

highly standardized[1545] and foreseeably causes physical harm.[1546] From a policy perspective, it is additionally argued that large software manufacturers dominating the market could absorb the costs.[1547] Courts have so far been more than reluctant to consider software itself a product for the purpose of tort liability.[1548] However, if software is integrated into a durable good (e.g. a car,[1549] cell phone,[1550] or video recording device[1551]), courts might be more willing to consider it (part of) a product.[1552]

[1545] *See, e.g.,* Shubha Ghosh & Vikram Mangalmurti, *Curing Cybersecurity Breaches Through Strict Products Liability*, *in* SECURING PRIVACY IN THE INTERNET AGE 187, 192 (Anupam Chander et al. eds., 2008). *But see* Patrick T. Miyaki, Comment, *Computer Software Defects: Should Computer Software Manufacturers Be Held Strictly Liable for Computer Software Defects?*, 8 SANTA CLARA COMPUTER & HIGH TECH. L.J. 121, 126 (1992) (arguing that software is more akin to services as it is often so complex that "it is impossible to test all the possible combinations of commands to make sure that [it] is defect free").

[1546] *See, e.g.,* Frances E. Zollers et al., *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 771 (2005).

[1547] *See, e.g.,* Shubha Ghosh & Vikram Mangalmurti, *Curing Cybersecurity Breaches Through Strict Products Liability*, *in* SECURING PRIVACY IN THE INTERNET AGE 187, 194 (Anupam Chander et al. eds., 2008); Frances E. Zollers et al., *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 771 (2005). *See generally* LEWIS BASS, PRODUCTS LIABILITY: DESIGN AND MANUFACTURING DEFECTS § 2:18 (2d ed. 2009).

[1548] *Cf.* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 19 (1998) (stating with regard to product liability for software that "there are no cases on point on the facts."); Seldon J. Childers, Note, *Don't Stop the Music: No Strict Products Liability for Embedded Software*, 19 U. FLA. J.L. & PUB. POL'Y 125, 142 (2008) (stating that diligent investigation has revealed no cases where judges have held that software was a product for purposes of tort products liability).

[1549] In Feb. 2010, due to a bug in the anti-lock break software, Toyota had to recall about 400,000 vehicles. *See* Blaine Harden & Frank Ahrens, *Toyota recalls more than 400,000 Priuses, other hybrid cars*, WASHINGTON POST, Feb. 10, 2010, at A12; Larry Dignan, *Toyota recalls: Is there a patch day for your car in the future?*, ZDNET, Feb. 23, 2010, http://blogs.zdnet.com/BTL/?p=31141.

[1550] When cell phones were still exclusively used for making phone calls, comparatively simple software was sufficient. The iPhone and other smart phones have, of course, created a new reality.

[1551] In many households, a TiVo, which is running a modified version of the Linux operating system, has replaced VCRs and DVD records. *Cf.* http://www.tivo.com/linux (last accessed Feb. 10, 2011).

[1552] *Cf.* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime,* 20 BERKELEY TECH. L.J. 1553, 1580 (2005).

Regarding the second element, a product defect, the plaintiff has to establish that the product: (1) contained a manufacturing defect; (2) was defective in design; or (3) was defective because of inadequate instructions or warnings.[1553]

Generally, a manufacturing defect is found to exist if the product deviates from the manufacturer's design.[1554] Many vulnerabilities (e.g. buffer overflows) could fall under this category as they are introduced in the implementation process and allow the software to be used contrary to its design.[1555] They are, however, different from conventional manufacturing defects, in the sense that they typically do not occur in "one in a million" units but rather in all or in none of the units,[1556] making them, in this respect, more akin to design defects.

A product is considered defective in design if a risk-benefit analysis leads to the conclusion that the design should have been avoided,[1557] or alternatively, under California law, the

[1553] *See* Hufft v. Horowitz, 5 Cal.Rptr.2d 377, 379 (Cal. Ct. App. 1992); Voss v. Black & Decker Mfg. Co., 450 N.E.2d 204, 207 (N.Y. 1983), *Cf.* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (1998).

[1554] Karlsson v. Ford Motor Co., 45 Cal.Rptr.3d 265, 270 (Cal. Ct. App. 2006) (holding that product is defectively manufactured if it contains some unintended flaw); Rainbow v. Albert Elia Bldg. Co., Inc., 436 N.Y.S.2d 480, 484 (N.Y. App. Div. 1981). *Cf.* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2(a) (1998) (stating that a product "contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product"). Under California law, a product is also defective if it "differs […] from other ostensibly identical units of the same product line." Barker v. Lull Eng'g Comp., Inc., 573 P.2d 443, 454 (Cal. 1978). In the context of standard software, however, all "units of the same product line" are identical copies, practically eliminating the possibility of any differences.

[1555] *See supra* chapter 3.1 (discussing different types of software vulnerabilities).

[1556] *Cf.* Seldon J. Childers, Note, *Don't Stop the Music: No Strict Products Liability for Embedded Software*, 19 U. FLA. J.L. & PUB. POL'Y 125, 139 (2008) (stating that the software manufacturing process has "no analogue to a traditional manufacturing process, and software defects do not appear in 'one in a million' configurations"); Shubha Ghosh & Vikram Mangalmurti, *Curing Cybersecurity Breaches Through Strict Products Liability*, *in* SECURING PRIVACY IN THE INTERNET AGE 187, 200 (Anupam Chander et al. eds., 2008) (only considering the software distribution process as part of manufacturing).

[1557] Barker v. Lull Eng'g Comp., Inc., 573 P.2d 443, 452 (Cal. 1978) (holding that the defendant has to prove that "on balance the benefits of the challenged design outweigh the risk of danger inherent in such design"). Voss v. Black & Decker Mfg. Co., 450 N.E.2d 204, 208 (N.Y. 1983) (holding that the proper standard is "whether it is a product which, if the design defect were known at the time of manufacture, a reasonable person would conclude that the utility of the product did not outweigh the risk inherent in marketing a product designed in that manner"). *Cf.* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2(b) (1998) (stating that a product failed to perform as safely as an ordinary consumer would expect when used in an intended or reasonably foreseeable manner.[1558] In particular the first standard might lead to significant uncertainties as the underlying technology can be very complex and the perceptions of risk and utility very subjective.[1559]

Under California law, a product is defective due to a "failure to warn" if it is "unreasonably dangerous" to place the product in the hands of consumers without a suitable warning and no warning is given.[1560] New York law requires a manufacturer to warn against "latent dangers resulting from foreseeable uses of its products of which it knew or should have known."[1561] California and New York law also require the manufacturer to provide a warning if dangerous properties of the product are discovered after the distribution to the customer.[1562] Software

product is defective in design "when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe").

[1558] Barker v. Lull Eng'g Comp., Inc., 573 P.2d 443, 454 (Cal. 1978). Under New York law, consumer expectations do not constitute an independent standard for judging the defectiveness of product designs. Tomasino v. Am. Tobacco Co., 807 N.Y.S.2d 603, 605 (N.Y. App. Div. 2005).

[1559] *Cf.* Shubha Ghosh & Vikram Mangalmurti, *Curing Cybersecurity Breaches Through Strict Products Liability*, *in* SECURING PRIVACY IN THE INTERNET AGE 187, 201 (Anupam Chander et al. eds., 2008) (noting that risk-utility balance may vary from individual to individual).

[1560] Canifax v. Hercules Powder Co., 46 Cal.Rptr. 552, 558 (Cal. Dist. Ct. App. 1965)

[1561] Rastelli v. Goodyear Tire & Rubber Co., 591 N.E.2d 222, 225 (N.Y. 1992). *Cf.* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2(b) (1998) (stating that a product is defective because of inadequate instructions or warnings "when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe").

[1562] This is, however, usually regarded as a form of negligence. *See* Torres v. Xomox Corp., 56 Cal. Rptr. 2d 455 (holding that "[w]hile strict liability for failing to warn extends only to risks which are 'known or knowable' when a product is sold […] a duty to warn may also arise if it is later discovered that the product has dangerous propensities, and breach of that duty is a form of negligence); Cover v. Cohen, 461 N.E.2d 864, 871 (N.Y. 1984) (holding that manufacturers may "incur liability for failing to warn concerning dangers in the use of a product which come to his attention after manufacture or sale, through advancements in the state of the art, with which he is expected to stay abreast, or through being made aware of later accidents"). *Cf.* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 10(a) (1998) (stating that "[o]ne engaged in the business of selling or otherwise distributing products is subject to liability for harm to persons or property caused by the seller's failure to manufacturers could therefore be required to warn of known security vulnerabilities present at the time of sale[1563] and to issue post-sale warnings for vulnerabilities discovered later on.[1564]

The third element to be established by the plaintiff is proximate cause which requires proving that the product defect was a "substantial factor" in the cause of the plaintiff's injury.[1565] This could be rather trivial in cases where a specific malware is found on the consumer's system and it can be proven that: (1) the malware only propagates by exploiting the product defect; and (2) the malware causes certain injuries. However, if no specific malware can be identified or if it also propagates by other ways than relying on the product defect, the common lack of digital evidence[1566] could make it very difficult to establish a causal link between the defect and the injury suffered by the plaintiff.

Lastly, the plaintiff needs to establish that she suffered recoverable damages. This is a very significant obstacle in most cases involving information security breaches as they typically only result in economic losses that are not recoverable unless physical injury occurs.[1567]

provide a warning after the time of sale or distribution of a product if a reasonable person in the seller's position would provide such a warning).

[1563] Due to the fact that new vulnerabilities are discovered in a very high frequency, particularly OEM software packages—which have a longer distribution time than downloadable software—often contain known security vulnerabilities at the time of sale.

[1564] A very efficient way of fulfilling these warning requirements is to provide an automatic security update installation process.

[1565] *See* Sindell v. Abbott Labs., 607 P.2d 924, 940 (Cal. 1980); Codling v. Paglia, 298 N.E.2d 622, 628 (N.Y. 1973).

[1566] *Cf.* DAN FARMER & WIETSE VENEMA, FORENSIC DISCOVERY 5 (2004) (discussing the volatility of many types of data that could be used as evidence).

[1567] San Francisco Unified School Dist. v. W.R. Grace & Co., 44 Cal.Rptr.2d 305 (holding that until physical injury occurs, that is, until damage rises above level of mere economic loss, plaintiff cannot state cause of action for strict liability or negligence); Bocre Leasing Corp. v. General Motors Corp., 645 N.E.2d 1195, 1199 (N.Y. 1995); Antel Oldsmobile-Cadillac, Inc. v. Sirus Leasing Co., 475 N.Y.S.2d 944, 945 (1984) (upholding dismissal of strict liability claim against manufacturer of computer that broke down and caused erasure of financial data because "the injury is properly characterized as 'economic loss' and plaintiff is relegated to

In summary, the strict liability theory of California and New York law, as it stands today, makes it next to impossible to recover economic losses suffered due to insecure software. Recovery might only be available for harm to persons or property if courts are willing to consider software a "product."

5.3.1.2. Negligence Tort Liability

Although product liability is typically based on strict tort liability,[1568] the tort of negligence can also be of relevance. Instead of having to establish the elements of defect, proximate cause, and injury, the plaintiff needs to prove the following elements: (1) duty, (2) breach of duty, (3) proximate causation, and (4) injury.[1569]

As these general requirements of a negligence claim have already been discussed *supra* in chapter 5.1.5.4, the following discussion will only focus on the peculiarities of negligence in the context of software product liability.

Many commentators have argued in favor of finding that software manufacturers have a duty towards licensees as well as towards third parties who might foreseeably be attacked by

contractual remedies"). *Cf.* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 21 (1998) (stating that "harm to persons or property includes economic loss if caused by harm to: (a) the plaintiff's person; or (b) the person of another when harm to the other interferes with an interest of the plaintiff protected by tort law; or (c) the plaintiff's property other than the defective product itself"). *Cf. also* Michael R. Maule, Comment, *Applying Strict Product Liability to Computer Software*, 27 TULSA L.J. 735, 745 (1992) (stating that the economic loss doctrine "is an important limit on the usefulness of strict products liability"); Peter A. Alces & Aaron S. Book, *When Y2K Causes "Economic Loss" to "Other Property"*, 84 MINN. L. REV. 1, 38 (1999) (discussing economic loss in the context of expected Y2K bug litigation). *Cf.* chapter 5.1.5.4 (discussing the economic loss doctrine in the context of negligence actions against personal information controllers).

[1568] *Cf.* VIVIAN S. CHU, CONG. RESEARCH SERV., PRODUCTS LIABILITY: A LEGAL OVERVIEW, CRS REPORT FOR CONGRESS, CRS REPORT FOR CONGRESS R40148, at 1 (2009), *available at* http://opencrs.com/document/R40148/2009-01-16/download/1013/.

[1569] *Cf.* 6 B.E. WITKIN, SUMMARY OF CALIFORNIA LAW, Torts § 835, at 52 (10th ed. 2005); Solomon v. City of New York, 489 N.E.2d 1294, 1294 (N.Y. 1985).

licensees' computer systems, once compromised.[1570] These arguments have been mostly based on the unique capability of manufacturers to address the underlying problems,[1571] and on general public policy considerations.[1572] As California and New York law does generally not require a plaintiff to establish privity, potential victims other then a licensee might have standing to sue.[1573]

However, the single most significant obstacle to any negligence claim against a software manufacturer is the economic loss doctrine which, as discussed *supra*, generally bars the recovery of economic losses absent harm to persons or property.[1574]

[1570] *See, e.g.,* Jennifer A. Chandler, *Improving Software Security: A Discussion of Liability for Unreasonably Insecure Software*, *in* SECURING PRIVACY IN THE INTERNET AGE 155, 163 (Anupam Chander et al. eds., 2008) (discussing a hypothetical negligence-based product liability claim of a victim of DDoS attack). The subsequent footnotes contain further references.

[1571] *See, e.g.,* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 444 (2008) (arguing that manufacturers of closed source software owe a duty to their licensees and to society as a whole to ensure the security of their software as they are the only ones who can isolate and repair problems).

[1572] *See, e.g.,* Erin Kenneally, *Stepping on the Digital Scale: Duty and Liability for Negligent Internet Security*, 26 ;LOGIN 62, 64 (2001) (arguing that "the costs associated with insecure computers on the Internet weigh heavily in favor of assigning a duty to secure systems"); Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1586 (2005) (proposing a new tort of negligent enablement of cybercrime, arguing that the epidemic of software vulnerabilities constitutes a compelling reason to recognize a new duty of reasonable internet security).

[1573] Greenman v. Yuba Power Prods., Inc., 377 P.2d 897 (Cal. 1963); Heller v. U.S. Suzuki Motor Corp., 477 N.E.2d 434, 437 (N.Y. 1985) (holding that consumers may maintain causes of action in New York to recover against both immediate and remote parties based on express or implied warranty, negligence or strict products liability). *Cf.* MORTON F. DALLER, PRODUCT LIABILITY DESK REFERENCE 68, 576 (2009).

[1574] Aas v. Superior Court, 12 P.3d 1125, 1130 (Cal. 2000) (holding that "[i]n actions for negligence, a manufacturer's liability is limited to damages for physical injuries; no recovery is allowed for economic loss alone"). Bocre Leasing Corp. v. General Motors Corp., 645 N.E.2d 1195, 1199 (N.Y. 1995) (holding that tort recovery in strict products liability and negligence against a manufacturer should not be available to a downstream purchaser where the claimed losses are economic losses such as damage to property that is the subject of the contract). *Cf.* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 21 (1998). *Cf.* Jennifer A. Chandler, *Improving Software Security: A Discussion of Liability for Unreasonably Insecure Software*, *in* SECURING PRIVACY IN THE INTERNET AGE 155, 166 (Anupam Chander et al. eds., 2008) (arguing that victims of DDoS attacks originating from customers' compromised computer systems should be allowed to recover economic losses as the number of foreseeable victims is small, thereby avoiding the problem of indeterminate liability).

5.3.2. Breach of Express or Implied Warranty under U.S. Law

In contrast to strict liability and negligence, a breach of warranty is not a tort but a claim based in contract law.[1575] Warranties are subject to the Magnuson-Moss Warranty Act (MMWA),[1576] article 2 of the Uniform Commercial Code (UCC),[1577] and, in California, the Song-Beverly Consumer Warranty Act.[1578] The Uniform Computer Information Transactions Act (UCITA), a model law only adopted by Maryland and Virginia, will not be discussed here.[1579]

The MMWA is a federal law that regulates written warranties on consumer products.[1580] As implemented by the rules promulgated by the FTC,[1581] it restricts "tie-in" conditions upon warranties[1582] and it mandates that the terms and conditions of a warranty be disclosed,[1583]

[1575] *Cf.* Windham at Carmel Mountain Ranch Ass'n v. Superior Court, 135 Cal. Rptr. 2d 834, 838 (Cal. Ct. App. 2003) (stating that "[a] warranty is a contractual term concerning some aspect of the sale, such as title to the goods, or their quality or quantity. The warranty may be express or implied.").

[1576] Magnuson-Moss Warranty Act, Pub. L. 93-637, 88 Stat. 2183 (1974) (codified at 15 U.S.C. §§ 2301-12).

[1577] The Uniform Commercial Code is a model law jointly developed by the National Conference of Commissioners on Uniform State Laws (NCCUSL) and the American Law Institute (ALI).

[1578] CAL. CIV. CODE § 1790 et seq. (West 2010).

[1579] UCITA was initially envisioned to be adopted as UCC art. 2b. When the ALI withdrew its support of the legislation, which was widely perceived as too "licensor-friendly," the NCCUSL changed the project's status from a UCC article to a freestanding uniform act. While Maryland and Virginia have adopted UCITA, other states have adopted so-called "bomb shelter" legislation, prohibiting courts from enforcing a contractual choice of law provision that selects a state in which UCITA is the governing law. *See* Maureen A. O'Rourke, *An Essay on the Challenges of Drafting a Uniform Law of Software Contracting*, 10 LEWIS & CLARK L. REV. 925, 929 (2006) (discussing UCITA's drafting process); Pratik A. Shah, *The Uniform Computer Information Transactions Act*, 15 BERKELEY TECH. L.J. 85, 86 (2000) (providing references to the comments and criticism UCITA received from industry groups, academics, consumer advocates, and governmental agencies).

[1580] *See generally* Christopher Smith, *The Magnuson-Moss Warranty Act: Turning The Tables on Caveat Emptor*, 13 CAL. WESTERN L. REV. 391 (1977); Kathleen F. Brickey, *The Magnuson-Moss Act – An Analysis of the Efficacy of Federal Warranty Regulation as a Consumer Protection Tool*, 18 SANTA CLARA L. REV. 73 (1978).

[1581] 40 Fed. Reg. 60,168 (Dec. 31, 1975) (codified at 16 C.F.R. § 701.1 et seq.).

[1582] *See* 15 U.S.C. § 2302(c).

[1583] *See* 15 U.S.C. § 2302(a); 16 C.F.R. § 701.3.

that the terms be made available to the consumer prior to the sale,[1584] that the warranty be designated as a "limited" or a "full" warranty,[1585] and that "full" warranties meet certain minimum requirements.[1586] Furthermore, the MMWA subjects disclaimers or modifications of implied warranties to restrictions.[1587] The substantive requirements of the MMWA are either rather easy to fulfill or easy to circumvent (by opting for a "limited" warranty). Moreover, its material scope of application is limited to the sale[1588] of "tangible personal property."[1589] This appears to drastically limit the extent to which MMWA applies to licensed software.[1590]

UCC article 2 which has been adopted in California[1591] and New York,[1592] *inter alia,* provides rules for implied and express warranties regarding the "sale" of "goods." Much of the debate has centered on the question of whether software is to be considered a "good." UCC § 2-105 defines "goods" as "all things (including specially manufactured goods) which are movable at

[1584] *See* 15 U.S.C. § 2302(b); 16 C.F.R. § 702.1-3.

[1585] *See* 15 U.S.C. § 2303.

[1586] *See* 15 U.S.C. § 2304.

[1587] Under 15 U.S.C. § 2308(a), a supplier may not disclaim or modify an implied warranty if (1) he makes a written warranty to the consumer, or (2) at the time of sale, or within 90 days thereafter, he enters into a service contract with the consumer. Implied warranties may, however, be limited in duration to the duration of a written warranty of reasonable duration. 15 U.S.C. § 2308(b).

[1588] *See* 15 U.S.C. § 2301(6) (defining "written warranty" as "(A) any written affirmation of fact or written promise made in connection with the *sale* of a consumer product […], or (B) any undertaking in writing in connection with the *sale* by a supplier of a consumer product to refund, repair, replace, or take other remedial action with respect to such product […]" (emphasis added)).

[1589] *See* 15 U.S.C. § 2301(1) (defining "consumer product" as "any tangible personal property which is distributed in commerce and which is normally used for personal, family, or household purposes"). *Cf.* Rebecca Crandall, Recent Development, *Do Computer Purchasers Need Lemon Aid?*, 4 N.C. J.L. & TECH. 307, 316 (2003).

[1590] Case law that would apply the MMWA to software licenses is non-existent.

[1591] CAL. COM. CODE § 2101 et seq. (West 2010).

[1592] N.Y. U.C.C. LAW § 2-101 et seq. (McKinney 2010).

the time of identification to the contract for sale […].”[1593] Many commentators have argued,[1594] and the majority of courts have found, that software, even when not bundled with computer hardware, is a “good.”[1595] Uncertainty remains, however, in particular with regard to software that is offered for download rather than distributed on a tangible medium.[1596]

[1593] *Cf.* CAL. COM. CODE § 2105(a); N.Y. U.C.C. LAW § 2-105(a).

[1594] *See* David R. Collins, *Shrinkwrap, Clickwrap, and Other Software License Agreements: Litigating a Digital Pig in a Poke in West Virginia*, 111 W. VA. L. REV. 531, 539 (2009); Jean Braucher, *Contracting Out of the Uniform Commercial Code: Contracting Out of Article 2 Using a "License" Label: A Strategy that Should Not Work for Software Products*, 40 LOY. L.A. L. REV. 261, 268 (2006) (arguing that software is considered tangible, i.e. fixed in a “tangible medium of expression,” for the purpose of copyright law and should therefore also be a good under UCC); Douglas E. Phillips, *When Software Fails: Emerging Standards of Vendor Liability Under the Uniform Commercial Code*, 50 BUS. LAW. 151, 158 (1994) (arguing that software is a good because the law of sales focuses on movability, not on tangibility); Bonna Lynn Horovitz, *Computer Software as a Good under the Uniform Commercial Code: Taking a Byte out of the Intangibility Myth*, 65 B.U.L. REV. 129, 151 (1985) (arguing that, considering the objectives of UCC art. 2, tangibility is not required and that software fulfills the requirements of “movability, transferability, and identification at the time of sale”); *But see* Edward G. Durney, *The Warranty of Merchantability and Computer Software Contracts: A Square Peg Won't Fit in a Round Hole*, 59 WASH. L. REV. 511, 516 (1984) (arguing that “movability” is designed to distinguish between real property and personal property and that software is intangible); Lorin Brennan, *Symposium on Approaching E-Commerce Through Uniform Legislation: Understanding the Uniform Computer Information Transactions Act and the Uniform Electronic Transactions Act: Why Article 2 Cannot Apply to Software Transactions*, 38 DUQ. L. REV. 459, 535 (2000) (arguing that software generally does not meet the “movability” test since it is copied rather than moved).

[1595] RRX Indus., Inc. v. Lab-Con, Inc., 772 F.2d 543, 546 (9th Cir. 1985) (holding that “employee training, repair services, and system upgrading were incidental to sale of the software package and did not defeat characterization of the system as a good”); Advent Sys. Ltd. v. Unisys Corp., 925 F.2d 670, 676 (3d Cir. 1991) (stating that “[t]he importance of software to the commercial world and the advantages to be gained by the uniformity inherent in the U.C.C. are strong policy arguments favoring inclusion” and holding that software is a “good” within the UCC); Softman Prods. Co. v. Adobe Sys., Inc., 171 F. Supp. 2d 1075, 1084 (C.D. Cal. 2001) (holding that “[a] number of courts have held that the sale of software is the sale of a good within the meaning of [UCC],” citing Advent Sys. Ltd. v. Unisys Corp., 925 F.2d 670, 676 (3d Cir. 1991); Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 99-100 (3rd Cir. 1991); and Downriver Internists v. Harris Corp., 929 F.2d 1147, 1150 (6th Cir. 1991)); Specht v. Netscape Commc'ns Corp., 150 F.Supp.2d 585, 591 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (2d Cir. 2002) (holding that the relationship between Netscape and the plaintiff how downloaded software from its website “essentially is that of a seller and a purchaser of goods,” subsequently applying “California law as it relates to the sale of goods, including the Uniform Commercial Code in effect in California”). Wachter Mgmt. Co. v. Dexter & Chaney, Inc., 144 P.3d 747, 750 (Kan. 2006) (holding that computer software is considered to be goods subject to the UCC even though incidental services are provided along with the sale of the software).

[1596] *Cf.* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 29 (2d Cir. 2002) (“Downloadable software, however, is scarcely a ‘tangible’ good, and, in part because software may be obtained, copied, or transferred effortlessly at the stroke of a computer key, licensing of such Internet products has assumed a vast importance in recent years. […] We need not decide today whether UCC Article 2 applies to Internet transactions in downloadable products.”); U.S. v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991) (holding that a “computer program itself is an intangible intellectual property, and as such, it alone cannot constitute stolen goods” within the meaning of 18 U.S.C. §§ 2314-2315).

Whether software transactions that take the form of a license can be considered a "sale" for the purpose of UCC article 2 has also been a much debated issue with most commentators advancing arguments for a liberal construction of article 2.[1597] UCC § 2-106(a) states that a sale "consists in the passing of title from the seller to the buyer for a price."[1598] Many courts have—rather than adopting a formalistic approach—focused on the economic realities of the transaction, often applying UCC article 2, at least by analogy, to software licenses.[1599]

If found to be applicable, article 2 provides rules for express as well as for implied warranties. Express warranties do not only include promises made within "the four corners of the

[1597] Jean Braucher, *Contracting Out of the Uniform Commercial Code: Contracting Out of Article 2 Using a "License" Label: A Strategy that Should Not Work for Software Products*, 40 LOY. L.A. L. REV. 261, 266 (2006) (arguing that UCC art. 2 works well enough if not perfectly for the issues it addresses and therefore, even if a court were to conclude that art. 2 does not apply directly to a license, it should apply by analogy); Bonna Lynn Horovitz, *Computer Software as a Good under the Uniform Commercial Code: Taking a Byte out of the Intangibility Myth*, 65 B.U.L. REV. 129, 139 (1985) (suggesting an application by analogy of UCC art. 2 to non-sale contracts); Andrew Rodau, *Computer Software: Does Article 2 of the Uniform Commercial Code Apply?*, 35 EMORY L.J. 853, 901 (1986) (arguing that software licenses are typically perpetual and therefore "equivalent to a sale since they are utilized, not to avoid a sale per se, but rather for purposes of copyright and protection of proprietary information"). *But see* Edward G. Durney, *The Warranty of Merchantability and Computer Software Contracts: A Square Peg Won't Fit in a Round Hole*, 59 WASH. L. REV. 511, 519 (1984) (arguing that the licensee does not receive all rights (i.e., title) to the software, therefore, no 'sale' occurs); Lorin Brennan, *Symposium on Approaching E-Commerce Through Uniform Legislation: Understanding the Uniform Computer Information Transactions Act and the Uniform Electronic Transactions Act: Why Article 2 Cannot Apply to Software Transactions*, 38 DUQ. L. REV. 459, 538 (2000) (arguing that the storage medium but not the software itself is sold because a non-exclusive software license does not involve a transfer of copyright ownership).

[1598] CAL. COM. CODE § 2106(1); N.Y. U.C.C. LAW § 2-106(1).

[1599] RRX Industries, Inc. v. Lab-Con, Inc., 772 F.2d 543, 546 (9th Cir. 1985) (holding the licensing of the software was a sale of goods under CAL. COM. CODE because "sales aspect [as opposed to the service aspect] of the transaction predominates"); ProCD, Inc., v. Zeidenberg, 86 F.3d 1447, 1450 (7th Cir. 1996) ("We treat the [database] licenses as ordinary contracts accompanying the sale of products, and therefore as governed by the common law of contracts and the Uniform Commercial Code."); SoftMan Prods. Co. v. Adobe Sys., Inc., 171 F. Supp. 2d 1075, 1084 (C.D. Cal. 2001) (stating that "[i]t is well-settled that in determining whether a transaction is a sale, a lease, or a license, courts look to the economic realities of the exchange," citing Applied Info. Mgmt., Inc. v. Icart, 976 F.Supp. 149, 155 (E.D.N.Y. 1997) and Microsoft Corp. v. DAK Indus., 66 F.3d 1091 (9th Cir.1995)); i.LAN Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 332 (D. Mass. 2002) (stating, in the context of a dispute between business parties, that "Article 2 technically does not, and certainly will not in the future, govern software licenses, but for the time being, the Court will assume that it does"). *Cf.* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 436 (2008) (noting that a majority of reported decisions have held that the fact that software is licensed does not preclude application of UCC art. 2). *See also* Stephen L. Sand, *Validity, Construction, and Application of Computer Software Licensing Agreements*, 38 A.L.R. 5TH 1, 20 (1996) (listing cases that recognized, either explicitly or by implication, that UCC art. 2 applies to computer software licenses).

contract," but also (1) "[a]ny affirmation of fact or promise made by the seller to the buyer which relates to the goods and becomes part of the basis of the bargain"; (2) "[a]ny description of the goods which is made part of the basis of the bargain"; and (3) "[a]ny sample or model which is made part of the basis of the bargain."[1600]

An implied warranty can be either one of merchantability or one of fitness for particular purpose. Under UCC § 2-314, a warrant of merchantability—which is only implied if the seller is a merchant with respect to the sold goods—requires that the goods pass without objection in the trade under the contract description and are fit for the ordinary purposes for which they are used.[1601] Pursuant to UCC § 2-315, a warranty of fitness for particular purpose is implied in a contract of sale if the seller, at the time of contracting, has reason to know any particular purpose for which the goods are required and that the buyer is relying on the seller's skill or judgment to select or furnish suitable goods.[1602]

However, these warranties remain without practical relevance to the extent that they are easily disclaimed or meaningful remedies for their breach are eliminated by contractual means.

UCC § 2-316(2) provides that implied warranties of merchantability can be disclaimed so long as the term "merchantability" is mentioned, and, if in writing, the exclusion is

[1600] UCC § 2-313(1)(a)-(c). *Cf.* CAL. COM. CODE § 2313(1)(a)-(c); N.Y. U.C.C. LAW § 2-313(1)(a)-(c). *Cf.* Robert A. Hillman, *U.C.C. Article 2 Express Warranties and Disclaimers In the Twenty-First Century*, 11 DUQ. BUS. L.J. 167, 168 (2009) (criticizing the "basis-of-the-bargain" test as failing to give meaningful guidance to transactors and courts).

[1601] *Cf.* CAL. COM. CODE § 2314; N.Y. U.C.C. LAW § 2-314.

[1602] *Cf.* CAL. COM. CODE § 2315; N.Y. U.C.C. LAW § 2-315. *Cf. also* Stephen E. Friedman, *Text and Circumstance: Warranty Disclaimers in a World of Rolling Contracts,* 46 ARIZ. L. REV. 677, 683 (2004) (discussing conditions under which implied warranties arise).

conspicuous.[1603] For implied warranties of fitness, the exclusion must be in writing and conspicuous.[1604]

Express warranties, on the other hand, cannot easily be disclaimed. Under UCC § 2-316(1), words or conduct relevant to the creation of an express warranty and words or conduct tending to negate a warranty are to be construed, where reasonable, "as consistent with each other."[1605] However, negation is "inoperative to the extent that such construction is unreasonable."[1606] Accordingly, most courts seem to favor express warranties over any disclaimer.[1607]

The UCC provides for a broad range of remedies, including direct damages for breach of warranty[1608] and incidental or consequential damages[1609] caused by the breach. However, the UCC provides that the agreement may "limit or alter the measure of damages […] as by

[1603] *Cf.* Robert W. Gomulkiewicz, *The Uniform Commercial Code Proposed Article 2B Symposium: The Implied Warranty of Merchantability in Software Contracts: A Warranty no One Dares to Give and How to Change That*, 16 J. MARSHALL J. COMPUTER & INFO. L. 393, 402 (1997) (noting that the implied warranty of merchantability of UCC art. 2 represents a well-intended but failed idea because it is disclaimed by virtually all software manufacturers; arguing that a different implied warranty, more accurately reflecting "commercial reality," would be less likely to be disclaimed).

[1604] UCC § 2-316(2); CAL. COM. CODE § 2316(2); N.Y. U.C.C. LAW § 2-316(2). *Cf. also* PAUL S. HOFFMAN, THE SOFTWARE LEGAL BOOK § 4.33 (2003) (noting that software vendors do, in fact, almost universally exclude implied warranties for the simple reason that no lawyer can confidently tell a vendor what the implied warranties mean when applied to software).

[1605] This language creates confusion as it asks a court to interpret statements as "consistent" that are indeed conflicting. *See* Robert A. Hillman, *U.C.C. Article 2 Express Warranties and Disclaimers In the Twenty-First Century*, 11 DUQ. BUS. L.J. 167, 170 (2009).

[1606] UCC § 2-316(1); CAL. COM. CODE § 2316(1); N.Y. U.C.C. LAW § 2-316(1).

[1607] *See* AM. L. INST., PRINCIPLES OF THE LAW OF SOFTWARE CONTRACTS, TENTATIVE DRAFT NO. 1 § 3.06, cmt. a (2008) and cases cited therein.

[1608] *See* UCC § 2-714(2) ("The measure of damages for breach of warranty is the difference at the time and place of acceptance between the value of the goods accepted and the value they would have had if they had been as warranted, unless special circumstances show proximate damages of a different amount."). *Cf.* CAL. COM. CODE § 2714(2); N.Y. U.C.C. LAW § 2-714(2).

[1609] *See* UCC § 2-715; CAL. COM. CODE § 2715; N.Y. U.C.C. LAW § 2-715.

limiting the buyer's remedies to return of the goods and repayment of the price or to repair and replacement of nonconforming goods or parts."[1610] Using this possibility, manufacturers of commercial off-the-shelf-software typically provide "return of the goods and repayment of the price" as the exclusive remedy.[1611] Consequential damages[1612] may be excluded, given that the exclusion is not unconscionable[1613]—which is presumed for "injury to the person in the case of consumer goods."[1614] However, there is no such presumption for damages where the loss is commercial.[1615]

In summary, UCC article 2 allows software manufacturers to disclaim all but express warranties and to limit the remedies to a full refund with the return of the software. Despite a

[1610] UCC § 2-719(1)(a); CAL. COM. CODE § 2719(1)(a); N.Y. U.C.C. LAW § 2-719(1)(a). *Cf.* UCC § 2-316(4) (stating that "[r]emedies for breach of warranty can be limited in accordance with [§§ 2-718, 2-719]"). *Cf. also* Douglas E. Phillips, *When Software Fails: Emerging Standards of Vendor Liability Under the Uniform Commercial Code*, 50 BUS. LAW. 151, 175 (1994).

[1611] Emily Kuwahara, *Torts v. Contracts: Can Microsoft Be Held Liable to Home Consumers For Its Security Flaws?*, 80 S. CAL. L. REV. 997, 1023 (2007) (noting that "[m]any consumers likely cannot function without Windows due to its virtual monopoly, so a full refund with the return of the product is a meaningless remedy").

[1612] Consequential damages include "any loss resulting from general or particular requirements and needs of which the seller at the time of contracting had reason to know and which could not reasonably be prevented by cover or otherwise." UCC § 2-715(2).

[1613] *Cf.* Armendariz v. Foundation Health Psychcare Service, Inc., 6 P.3d 669, 690 (Cal. 2000) (holding that unconscionability has both a procedural and a substantive element, the former focusing on oppression or surprise due to unequal bargaining power, the latter on overly harsh or one-sided results; the prevailing view is that procedural and substantive unconscionability must both be present but they need not be present in the same degree); Sablosky v. Edward S. Gordon Co., Inc., 535 N.E.2d 643, 647 (N.Y. 1989) (holding that the doctrine of unconscionability contains both substantive and procedural aspects, and whether contract or clause is unconscionable is to be decided by court against background of contract's commercial setting, purpose, and effect).

[1614] UCC § 2-719(3); CAL. COM. CODE § 2719(3); N.Y. U.C.C. LAW § 2-719(3).

[1615] *Cf.* Daniel T. Perlman, Notes and Comments, *Who Pays the Price of Computer Software Failure?*, 24 RUTGERS COMPUTER & TECH. L.J. 383, 392 (1998) (noting that a commercial purchaser that is not allowed to recover consequential damages may suffer a substantial economic loss).

limitation of remedies, consequential damages might be available for "injury to the person in the case of consumer goods" but not for economic losses.[1616]

In California, the Song-Beverly Consumer Warranty Act[1617] (hereinafter *Song-Beverly Act*) provides an additional regime for warranties for the "sales"[1618] of "consumer goods"[1619] in California.[1620] To the extent that the Song-Beverly Act gives rights to the buyers, it prevails over conflicting provisions of the UCC.[1621] Analogous to the UCC, it seems likely that the licensing of software would also be considered a "sale" of "consumer goods" under the Act.[1622]

The Song-Beverly Act provides requirements for the creation and exclusion of express warranties[1623] as well as for implied warranties of merchantability[1624] and implied warranties

[1616] Note that under UCC § 2-318, a warranty—whether express or implied—extends to "any natural person if it is reasonable to expect that such person may use, consume or be affected by the goods and *who is injured in person* by breach of the warranty" (emphasis added). This provision was adopted in New York but not in California. N.Y. U.C.C. LAW § 2-318.

[1617] CAL. CIV. CODE § 1790 et seq. (West 2010).

[1618] CAL. CIV. CODE § 1791(n) (defining the term "sale" as either the "passing of title from the seller to the buyer for a price" or "[a] consignment for sale").

[1619] CAL. CIV. CODE § 1791(a) (defining the term "consumer goods" as "any new product or part thereof that is used, bought, or leased for use primarily for personal, family, or household purposes […]").

[1620] *Cf.* Annunziato v. eMachines, Inc., 402 F. Supp. 2d 1133, 1142 (purchaser's Song-Beverly Act claim was subject to dismissal because the purchaser failed to allege an in-state purchase).

[1621] *See* CAL. CIV. CODE § 1790.3 (stating that "where the provisions of the Commercial Code conflict with the rights guaranteed to buyers of consumer goods under the provisions of this chapter, the provisions of this chapter shall prevail").

[1622] *Cf.* Jeffrey C. Selman & Christopher S. Chen, *Steering the Titanic Clear of the Iceberg: Saving the Sale of Software From the Perils of Warranties*, 31 U.S.F. L. REV. 531, 540 (1997) (stating that the Act "applies to the sale of any computer hardware or software product used for any one of the stated purposes"); KATHERYN A. ANDRESEN, 1 LAW AND BUSINESS OF COMPUTER SOFTWARE § 18:20 (2d ed. 2009). Courts have yet to decide on the issue.

[1623] *See* CAL. CIV. CODE § 1791.2(a) (defining "express warranty" as "[a] written statement arising out of a sale […] pursuant to which the manufacturer, distributor, or retailer undertakes to preserve or maintain the utility or performance of the consumer good or provide compensation if there is a failure in utility or performance"; or "[i]n the event of any sample or model, that the whole of the goods conforms to such sample or model"). *See also* CAL. CIV. CODE § 1793.1 (providing further requirements regarding the form of express warranties).

of fitness.[1625] Both types of implied warranties apply to manufacturers as well as retail sellers.[1626]

However, all implied warranties can be disclaimed if a conspicuous writing is attached to the goods which clearly informs the buyer, prior to the sale, "in simple and concise language"[1627] that (1) the goods are being sold on an "as is" or "with all faults" basis; (2) the entire risk as to the quality and performance of the goods is with the buyer; (3) should the goods prove defective following their purchase, the buyer assumes the entire cost of all necessary servicing or repair.[1628]

Equally important, the Song-Beverly Act provides that remedies for a breach of implied warranties can be limited in accordance with the requirements under UCC article 2.[1629] This allows software manufacturers to limit the remedies to repair and replacement or a full refund

[1624] *See* CAL. CIV. CODE § 1791.1(a) (stating that an implied warranty of merchantability, *inter alia*, requires that the goods "[p]ass without objection in the trade under the contract description" and "[a]re fit for the ordinary purposes for which such goods are used").

[1625] *See* CAL. CIV. CODE § 1791.1(a) (stating that an implied warranty of fitness mans "that when the retailer, distributor, or manufacturer has reason to know any particular purpose for which the consumer goods are required, and further, that the buyer is relying on the skill and judgment of the seller to select and furnish suitable goods, then there is an implied warranty that the goods shall be fit for such purpose […]").

[1626] *See* CAL. CIV. CODE § 1792 ("Unless disclaimed in the manner prescribed by this chapter, every sale […] shall be accompanied by the manufacturer's and the retail seller's implied warranty that the goods are merchantable"); *Id.* § 1792.1 (manufacturer's implied warranty of fitness for particular purpose); *Id.* § 1792.2 (retailer's or distributor's implied warranty of fitness for particular purpose).

[1627] CAL. CIV. CODE § 1792.4(a).

[1628] *Id.* § 1792.4(a)(1)-(3). *Cf. id.* § 1792.5 (stating that all sales on an "as is" or "with all faults" basis, made in compliance with the provisions of this chapter, shall constitute a waiver by the buyer of the implied warranty of merchantability and, where applicable, of the implied warranty of fitness).

[1629] CAL. CIV. CODE § 1791.1(d) (referring to CAL. COM. CODE § 2719). *See supra.*

with the return of the software[1630] and to exclude consequential damages where they do not involve "injury to the person."[1631]

5.3.3. Product Liability Under the EU Product Liability Directive

The issue of product liability has, to a significant extent, been harmonized by the adoption of Council Directive 85/374[1632] (hereinafter *Product Liability Directive*).

Under article 1 of the Product Liability Directive, a "producer" is liable for "damage" caused by a "defect" in his "product" whereas an injured person is required to prove the damage, the defect, and the causal relationship between defect and damage.[1633]

5.3.3.1. Software as a "Product"

Regarding the potential liability of software manufacturers, the meaning of the term "product" is of primary significance. It is defined in article 2 as "all movables even if incorporated into another movable or into an immovable" and "includes electricity."[1634] The first decisive question therefore is whether software is to be a considered a product under the Product Liability Directive. Since the ECJ has so far not addressed the issue, there is considerable disagreement in the literature.

[1630] CAL. COM. CODE § 2719(1)(a).

[1631] CAL. COM. CODE § 2719(3).

[1632] 1985 O.J. (L 210) 29 (EEC) as amended by Parliament and Council Directive 1999/34, 1999 O.J. (L 141) 20 (EC).

[1633] *See* Product Liability Directive art. 4.

[1634] Note that Product Liability Directive art. 2, before it was amended by Parliament and Council Directive 1999/34, art. 1, 1999 O.J. (L 141) 20, 21 (EC), explicitly excluded "primary agricultural products and game."

If a good that is put into circulation consists of software and of a machine or electronic device into which the software is integrated (e.g. a PC with a pre-installed operating system or a printer with firmware), the software is commonly considered part of the product.[1635]

Less clear are cases in which the software is only combined with a physical medium (e.g. a CD) in order to facilitate the circulation of the software. While some argue that this makes software a "movable,"[1636] others note that the immaterial aspect of "software on a CD" would still be dominant.[1637]

Moreover, entirely unsettled is the question whether software is a product, if it is not distributed on a physical medium but made available over the Internet[1638]:

[1635] *See* Axel Bauer, *Produkthaftung für Software nach geltendem und künftigem deutschen Recht* [*Product Liability for Software Under Current and Future German Law*], 1989 PRODUKTHAFTPFLICHT INTERNATIONAL 39, 43 (F.R.G.); Kurt Mayer, *Das neue Produkthaftungsrecht* [*The New Product Liability Law*], 1990 VERSICHERUNGSRECHT 691, 695, 697 (F.R.G.). HANS JOSEF KULLMANN, PRODUKTHAFTUNGSGESETZ [PRODUCT LIABILITY ACT] 82 (3d ed. 2001); ANDREAS EUSTACCHIO, PRODUKTHAFTUNG: EINE SYSTEMATISCHE DARSTELLUNG FÜR DIE PRAXIS [PRODUCT LIABILITY: A PRACTICAL SYSTEMATIC OUTLINE] 34 (2002); ANDREAS GÜNTHER, PRODUKTHAFTUNG FÜR INFORMATIONSGÜTER [PRODUCT LIABILITY FOR INFORMATION GOODS] 189 (2001) (with further references). A typical example of an integrated software would be a laptop that explodes due to a defect in the Basic Input/Output System (BIOS). Note, however, that there is no consensus with regard to the question of whether a firmware is an independent product. *Cf. id.* at 190 (with further references).

[1636] Diane Rowland, *Liability for Defective Software*, 22 CAMBRIAN L. REV. 78 (1991); HANS JOSEF KULLMANN, PRODUKTHAFTUNGSGESETZ [PRODUCT LIABILITY ACT] 83 (3d ed. 2001); Chris Reed & Alison Welterveden, *Liability, in* COMPUTER LAW 87, 98 (Chris Reed & John Angel eds., 4th ed. 2000); Stephen J. Saxby, *Liability for On-line Data Bank Services in the United Kingdom*, *in* LIABILITY FOR ON-LINE DATA BANK SERVICES IN THE EUROPEAN COMMUNITY 321, 278 (Ulrich Sieber ed., 1992). *Cf. also* ANDREAS GÜNTHER, PRODUKTHAFTUNG FÜR INFORMATIONSGÜTER [PRODUCT LIABILITY FOR INFORMATION GOODS] 193 (2001).

[1637] *Cf.* HANS CLAUDIUS TASCHNER & EDWIN FRIETSCH, PRODUKTHAFTUNGSGESETZ UND EG-PRODUKTHAFTUNGSRICHTLINIE [PRODUCT LIABILITY ACT AND EC PRODUCT LIABILITY DIRECTIVE] 305 (2d ed. 1990); HANS-WERNER MORITZ & BARBARA TYBUSSECK, COMPUTERSOFTWARE [COMPUTER SOFTWARE] § 920 (2d ed. 1992); Axel Bauer, *Produkthaftung für Software nach geltendem und künftigem deutschen Recht (Teil 2)* [*Product Liability for Software Under Current and Future German Law (Part 2)*], 1989 PRODUKTHAFTPFLICHT INTERNATIONAL 98, 102 (F.R.G.).

[1638] *Cf.* AXEL SODTALBERS, SOFTWAREHAFTUNG IM INTERNET [SOFTWARE LIABILITY ON THE INTERNET] 105 (2006) (explaining that this question is unsettled because the drafters of the Product Liability Directive simply did not think of the possibility that software could also be a product).

Proponents of software product liability can refer to an answer given by the Commission in 1989 to a question from the European Parliament in which the Commission—in an effort to diffuse calls for new legislation on software product liability—explicitly stated, albeit without reasoning, that "the Directive applies to software."[1639]

This statement by the Commission is, however, not binding on the ECJ or the Member States. Furthermore, it should be pointed out that the Commission did not initiate infringement procedures against Member States that explicitly limited product liability to "tangible" movables.[1640] In subsequent publications, the Commission also seems to have reversed itself: in its 1999 Green Paper on liability for defective products as well as in its second report on the application of the Product Liability Directive,[1641] the Commission explicitly defined the Directive's scope as "*material* movables […] including electricity"[1642] (emphasis added).

It has been argued that software should be treated analogous to electricity which is also not a "movable" but nevertheless explicitly covered by the Directive.[1643] However, the contrary

[1639] Answer given by Lord Cockfield on behalf of the Commission to Written Question No 706/88 by Mr. Gijs de Vries (LDR–NL), 1989 O.J. (C 114) 42. *Cf.* CHRISTIAN HORWATH, SOFTWARE UND PRODUKTHAFTUNG [SOFTWARE AND PRODUCT LIABILITY] 47 (2002).

[1640] For example Belgium restricted the definition of product to "tangible" movables. *See* Belgisch Staatsblad, Mar. 22, 1991, at 5884. *Cf.* LOVELLS, PRODUCT LIABILITY IN THE EUROPEAN UNION: A REPORT FOR THE EUROPEAN COMMISSION 78 (2003), *available at* http://ec.europa.eu/enterprise/policies/single-market-goods/files/goods/docs/liability/studies/lovells-study_en.pdf.

[1641] Pursuant to Product Liability Directive art. 21, the Commission has to present every five years a report to the Council on the application of the Directive and, if necessary, has to submit appropriate proposals to it.

[1642] Commission Green Paper, Liability for defective products, at 30, COM (1999) 396 final (July 28, 1999); Report from the Commission on the Application of Directive 85/374 on Liability for Defective Products, at 24, COM (2000) 893 final (Jan. 31, 2001).

[1643] Friedrich Graf von Westphalen, *Das deutsche Produkthaftungsgesetz* [*The German Product Liability Act*], *in* 2 PRODUKTHAFTUNGSHANDBUCH [2 PRODUCT LIABILITY HANDBOOK] 68 (Friedrich Graf von Westphalen ed., 1999); Jürgen Taeger, *Produkt- und Produzentenhaftung bei Schäden durch fehlerhafte Computerporgramme* [*Product and Producer Liability for Damages Caused by Faulty Computer Programs*], 1996 COMPUTER UND RECHT 257, 261 (F.R.G.) (arguing that software is a movable because it had to be stored on a material medium at any time). Some also argue that the object and purpose of the Directive requires the inclusion of software since it was a commercial good like any other. *See* Michael Lehmann, *Produkt- und Produzentenhaftung für Software* argument can also be made: since the EU legislator named only one exception (electricity) to the general rule that only "movables" are covered, it did not intend software to be covered.[1644]

Ultimately, the issue of whether software can be generally considered a product under the Product Liability Directive will only be settled by the ECJ.

5.3.3.2. Persons Liable

As stated above, only a "producer" is liable under the Product Liability Directive. Article 3(1) defines this term broadly as "the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer."[1645] To ensure that an injured person is effectively able to get compensation in cases of products that were manufactured outside of the EU, the Directive provides that—without prejudice to the liability of the actual producer—any person who imports into the EU a product for distribution in the course of his business shall be deemed a producer.[1646] Furthermore, if the producer cannot be identified,[1647] each supplier of the product shall be treated as its producer

[*Product and Producer Liability for Software*], 1992 NEUE JURISTISCHE WOCHENSCHRIFT 1721, 1724 (F.R.G.); Michael Kort, *Produkteigenschaft medizinischer Software: Einordnung im deutschen und US-amerikanischen Produkthaftungsrecht* [*Medical Software as Products: Classification Under German and U.S. Product Liability Law*] 1990 COMPUTER UND RECHT 171, 174 (F.R.G.).

[1644] *Cf.* HANS JOSEF KULLMANN, PRODUKTHAFTUNGSGESETZ [PRODUCT LIABILITY ACT] 84 (3d ed. 2001); ANDREAS GÜNTHER, PRODUKTHAFTUNG FÜR INFORMATIONSGÜTER [PRODUCT LIABILITY FOR INFORMATION GOODS] 200 (2001) (with further references).

[1645] Product Liability Directive art. 3(1).

[1646] *See* Product Liability Directive art. 3(2).

[1647] *Cf.* Case C-402/03, Skov Æg v. Bilka Lavprisvarehus A/S, 2006 E.C.R. I-199, §§ 33-37 (holding that Member States may not make suppliers liable if the producer can be identified).

unless he informs the injured person of the identity of the producer or of the person who supplied him with the product.[1648]

As regards software, this liability regime effectively guarantees that an injured person can sue somebody in the EU—that is if the software was distributed on a tangible medium. If it was, however, directly downloaded over the Internet from a software manufacturer outside of the EU, there is no supplier and no importer to turn to.[1649] In such cases, an injured person may only claim damages from the actual producer.[1650]

5.3.3.3. Product Defects

According to article 6 of the Product Liability Directive, a product is defective "when it does not provide the safety which a person is entitled to expect, taking all circumstances into account." The circumstances that are to be considered include (1) the presentation of the

[1648] *See* Product Liability Directive art. 3(3). *Cf.* Case C-358/08, Aventis Pasteur SA v. OB, 2009 ECJ EUR-Lex LEXIS 1103, § 57-58 (holding that it is not sufficient to only deny being the producer; the supplier has to inform the plaintiff "on its own initiative and promptly, of the identity of the producer or its own supplier"). *Cf. also* SUSANNE HILL-ARNING & WILLIAM C. HOFFMAN, PRODUKTHAFTUNG IN EUROPA [PRODUCT LIABILITY IN EUROPE] 14 (1995) and Ferdinando Albanese, *Legal Harmonisation in Europe, Product Liability: A Comparison Between the Directive of the European Communities and the Council of Europe Convention*, *in* COMPARATIVE PRODUCT LIABILITY 15, 20 (C. J. Miller ed., 1986) (discussing the advantages of subsidiary liability for a potential plaintiff).

[1649] The Internet access provider the services of which were used to download the software cannot be considered a supplier or importer. It did neither profit from the transaction nor would it be able to correct the software's defect.

[1650] For defendants who are not domiciled in a Member State, jurisdiction is to be determined by the law of the Member State in which the suit is brought. *See* Council Regulation, art. 4(1), 2001 O.J. (L 12) 1, 4 (EC) (referring to art. 22 and 23 which list the only cases in which a Member State has to assert jurisdiction over a defendant domiciled outside of the EU). *Cf.* PIRMIN BISCHOF, PRODUKTHAFTUNG UND VERTRAG IN DER EU [PRODUCT LIABILITY AND CONTRACT IN THE EU] 88 (1994) (criticizing the extent of flexibility given to Member States). The applicable law is to be determined under Parliament and Council Regulation 864/2007, art. 5, 2007 O.J. (L 199) 40, 44 (EC). The question of whether the judgment can be enforced in the U.S. is, however, another matter.

product, (2) the use to which the product could reasonably be expected to be put, and (3) the time when the product was put into circulation.[1651]

An example of a software product defect that is discussed in the literature and occasionally occurs in practice is that software is distributed with malware that infected the software at some point in the software manufacturing process.[1652] It was argued that a malware infection only constituted a defect if the malware was known—and therefore detectable by anti-malware software—at the time of distribution.[1653] However, since software manufacturers can generally be expected to perform a review of the source code before releasing the software, all malware infections should be regarded as a defect.[1654]

Another example is anti-malware software that incorrectly identifies legitimate files as malware (referred to as false positives).[1655] If the anti-malware software automatically deletes the incorrectly identified file, the stability of the entire operating system may be affected.

[1651] *See* Product Liability Directive art. 6(1)(a)-(c).

[1652] *See, e.g.,* Dancho Danchev, *Vodafone HTC Magic shipped with Conficker, Mariposa malware*, ZDNET, Mar. 9, 2010, http://www.zdnet.com/blog/security/vodafone-htc-magic-shipped-with-conficker-mariposa-malware/5626; Thomas Claburn, *Energizer Removes Infected Battery Monitoring Software*, INFORMATIONWEEK, Mar. 8, 2010, *available at* http://www.informationweek.com/news/hardware/desktop/showArticle.jhtml?articleID=223200155; Deborah Gage, *Popular photo frames carry risk of infection*, SAN FRANCISCO CHRONICLE, Jan. 2, 2009, at C1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/01/02/BUV9150IH8.DTL; Ryan Naraine, *Malware found in Lenovo software package*, ZDNET, Nov. 19, 2008, http://www.zdnet.com/blog/security/malware-found-in-lenovo-software-package/2203.

[1653] Günter Freiherr von Gravenreuth, *Computerviren und Haftung des Arbeitnehmers* [*Computer Viruses and Employee Liability*], SICHERHEITS-BERATER, Apr. 1993, Supp., at 2, 4 (F.R.G.).

[1654] *See* JÜRGEN TAEGER, AUßERVERTRAGLICHE HAFTUNG FÜR FEHLERHAFTE COMPUTERPROGRAMME [NON-CONTRACTUAL LIABILITY FOR DEFECTIVE COMPUTER PROGRAMS] 178 (1995). *Cf. also* ANDREAS GÜNTHER, PRODUKTHAFTUNG FÜR INFORMATIONSGÜTER [PRODUCT LIABILITY FOR INFORMATION GOODS] 211 (2001).

[1655] *Cf.* John Leyden, *Rogue McAfee update strikes police, hospitals and Intel*, THE REGISTER, Apr. 22, 2010, http://www.theregister.co.uk/2010/04/22/mcafee_false_positive_analysis/ (discussing that many enterprises, including police departments and hospitals in the US, were hit by a false positive from McAfee on Wednesday that labeled a core Windows file as potentially malign); Gregg Keizer, *Symantec false positive cripples thousands of Chinese PCs*, COMPUTERWORLD, May 18, 2007, http://www.computerworld.com/s/article/9019958/Symantec_false_positive_cripples_thousands_of_Chinese_PCs; JOHN VIEGA, THE MYTHS OF SECURITY: WHAT THE COMPUTER SECURITY INDUSTRY DOESN'T WANT YOU TO KNOW 44 (2009) (describing how McAfee in 2006 released an update that detected Microsoft Excel as a virus and deleted it from machines).

Since a person is "entitled to expect" that anti-malware software does not damage the underlying operating system, such characteristics of an anti-malware software are clearly a defect.[1656]

One further example is the ineffectiveness of security software such as a firewall or an anti-malware software. However, there has been a considerable amount of debate about whether ineffectiveness should be considered a defect, given that the Directive states that defectiveness of a product "should be determined by reference not to its fitness for use but to the lack of the safety."[1657] However, a differentiation between defectiveness and ineffectiveness is often elusive or even impossible.[1658] Like a helmet that is distributed with a hairline crack or a seatbelt that breaks under stress,[1659] security software that does not perform its security function should be considered defective.

An issue that directly affects information security and is much more significant in practice than the issues discussed above—but rarely discussed in the literature—is whether and to what extent security vulnerabilities can be considered defects.

[1656] *Cf. infra* chapter 5.3.3.4 (discussed that the software manufacturer may have a defense under art. 7(b) if the defect was introduced by an update).

[1657] Product Liability Directive recital 6. *Cf.* HANS CLAUDIUS TASCHNER & EDWIN FRIETSCH, PRODUKTHAFTUNGSGESETZ UND EG- PRODUKTHAFTUNGSRICHTLINIE [PRODUCT LIABILITY ACT AND EC PRODUCT LIABILITY DIRECTIVE] 306 (2d ed. 1990); RUDOLF WELSER & CHRISTIAN RABL, PRODUKTHAFTUNGSGESETZ [PRODUCT LIABILITY ACT] § 5 recital 46 (2d ed. 2004).

[1658] For example, is the break of a car ineffective or defective if it does not work? One could argue that the car is defective while the break is only ineffective. This would, however, lead to the nonsensical conclusion that the car manufacturer is liable while the manufacturer of the break is not. *See* Gottfried Musger, *Zur Anwendung des PHG auf wirkungslose Produkte* [*Application of the Product Liability Act to Ineffective Products*], 1990 WIRTSCHAFTSRECHTLICHE BLÄTTER 289 (Austria); HANNS FITZ ET AL, PRODUKTHAFTUNG [PRODUCT LIABILITY] § 5 recital 128 (2004). *Cf. also* HANS JOSEF KULLMANN, PRODUKTHAFTUNGSGESETZ [PRODUCT LIABILITY ACT] 114 (3d ed. 2001); MATHIAS HABERSACK ET AL., 5 MÜNCHNER KOMMENTAR ZUM BÜRGERLICHEN GESETZBUCH [5 MUNICH COMMENTARY OF THE CIVIL CODE] ProdHaftG § 4 recital 37 (Franz Jürgen Säcker & Roland Rixecker eds., 5th ed. 2009) (explicitly noting that anti-virus software is defective if it does not protect from viruses).

[1659] HANNS FITZ ET AL, PRODUKTHAFTUNG [PRODUCT LIABILITY] § 5 recital 128 (2004) (naming parachutes and life jackets as further examples).

Since software is generally known to contain many security vulnerabilities, users of the software product are not "entitled to expect" vulnerability-free software. For example, 70 "highly severe"[1660] security vulnerabilities affecting the popular browser Mozilla Firefox were publicly disclosed between September 1, 2009 and August 31, 2010.[1661] However, this is not to say that all types of vulnerabilities are to be expected. Some vulnerabilities, through a combination of their severity and ease with which they could have been prevented, are not to be expected.[1662]

For example, users are generally entitled to expect that software does not contain any "backdoors" that allow unauthorized access by malicious threat agents. Backdoors allow the circumvention of normal authentication procedures and are typically built into software to facilitate testing during development but are sometimes forgotten and therefore not removed before the software is distributed.[1663] Alternatively, backdoors may be created for malicious

[1660] As used in this thesis, "highly severe" refers to a CVSS Version 2 Severity Base Score Range of 7 to 10. *Cf.* Peter Mell et al., *Common Vulnerability Scoring System*, IEEE SECURITY & PRIVACY, Nov. 2006, at 85, 86 ("The base metrics represent the vulnerability's immutable characteristics (properties that are constant over time and across systems). They produce a score within the range of 0.0 to 10.0"). *Cf.* http://web.nvd.nist.gov/view/vuln/search-advanced?cid=9 (referring to the base score range of 7 to 10 as "High").

[1661] This data can be obtained using the National Vulnerability Database's advanced search functionality. *See* http://web.nvd.nist.gov/view/vuln/search-advanced?cid=9 (last accessed Feb. 10, 2011).

[1662] *Cf.* CHRISTIAN HORWATH, SOFTWARE UND PRODUKTHAFTUNG [SOFTWARE AND PRODUCT LIABILITY] 104 (2002) (emphasizing that some defects can indeed be prevented).

[1663] Backdoors that are created for development purposes are sometimes also referred to as "maintenance hooks." *See* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 382 (4th ed. 2008) (noting that maintenance hooks are not a thing of the past; they are still used by developers "because of their lack of understanding or care of security issues"). In particular BIOS manufacturers are known to regularly use backdoor passwords. *See* QUENTIN DOCTER ET AL., COMPTIA A+ COMPLETE STUDY GUIDE 574 (2009). *Cf. also* Ed Skoudis, *Hacker Tools and Techniques, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 935, 946 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007). A backdoor that consisted of a built-in hidden account was also famously used in the movie WARGAMES (Metro-Goldwyn-Mayer 1983).

reasons by developers as well as by outsiders that manage to compromise the code repository.[1664]

As far as commercial off-the-shelf software (COTS) is concerned, most types of vulnerabilities other than backdoors will unfortunately have to be expected. This is due to the fact that the long history of software vulnerabilities has arguably led to a reduced level of expectations to which users are entitled.[1665] Ironically, the more common and therefore the more significant a specific type of vulnerability is, the less users will be entitled to expect that such types of vulnerabilities are not present in software. For example, most of the vulnerability types that can be found on the 2010 list of the 25 most dangerous software vulnerabilities as compiled by the SANS Institute and the MITRE Corporation[1666] are indeed very common and therefore to be expected to be present in COTS.[1667]

The expectations a user is entitled to have may, however, differ with regard to special purpose software that is reasonable to be used in high-risk situations such as for medical purposes, to control a car, or to manage the electrical grid. For such software, the CWE/SANS Top 25

[1664] *Cf., e.g.,* Kevin Poulsen, *Thwarted Linux backdoor hints at smarter hacks*, SECURITYFOCUS, Nov. 6, 2003, http://www.securityfocus.com/news/7388.

[1665] *Cf.* ANDREAS GÜNTHER, PRODUKTHAFTUNG FÜR INFORMATIONSGÜTER [PRODUCT LIABILITY FOR INFORMATION GOODS] 209 (2001) (with further references).

[1666] SANS INST. & MITRE CORP., 2010 CWE/SANS TOP 25 MOST DANGEROUS SOFTWARE ERRORS (2010), *available at* http://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.pdf.

[1667] The top four vulnerability types are cross-site scripting (CWE-79), SQL injection (CWE-89), classic buffer overflows (CWE-120), and cross-site request forgery (CWE-352). Three of those four are particularly common. Of the 4,948 CVEs registered between Sept. 1, 2009 and Aug. 31, 2010, 733 (14.8%) were cross-site scripting vulnerabilities, 658 (13.3%) were SQL injection vulnerabilities, 560 (11.3%) were buffer errors, and 91 (1.8%) were cross-site request forgery vulnerabilities. This data is available via the National Vulnerability Database's advanced search functionality. *See* http://web.nvd.nist.gov/view/vuln/search-advanced?cid=9 (last accessed Sept. 8, 2010).

Most Dangerous Software Errors might indeed be a good starting point for determining the safety a person is "entitled to expect."[1668]

Another issue that challenges the conception of security vulnerabilities as product defects is that products do not have to be safe for "any misuse of the product not reasonable under the circumstances."[1669] Is the attempt of a criminal to compromise a computer system by exploiting a vulnerability in the software product an unreasonable misuse of the software for which the producer does not have to ensure safety?

A comparison to the product liability for cars is helpful: Is it reasonable that a car is used in a head-on collision with a ghost driver's car (who may or may not act intentionally)? There is a general consensus that, while the car was certainly not intended to be used in that way, it is a regularly occurring "use" which has to be taken into account when manufacturing a car.[1670]

Similarly, software is generally not intended to be the target of hacking attempts. It is, however, typically intended to be used on a computer that is connected to the Internet. As such the software will likely be exposed to countless efforts that aim at finding and exploiting vulnerabilities in that software. Accordingly, using software in a way that exposes it to attacks is a use that "could reasonably be expected."[1671]

[1668] Note that the SANS Institute and the MITRE Corp. cooperated with experts from more than 30 U.S. and international cyber security organizations to develop this list, *inter alia*, with the objective of establishing a baseline for liability. *See* Press Release, SANS Inst., New Top 25 Software Errors Opens Door to Shift Liability for Faulty Code from Buyers to Developers (Feb. 16, 2010), *available at* http://www.sans.org/top25-software-errors/press-release.php.

[1669] Product Liability Directive recital 6. *Cf. also* Product Liability Directive art. 6(1)(b) (requiring to take into account "the use to which it could reasonably be expected that the product would be put").

[1670] *See* JOACHIM SCHMIDT-SALZER, 1 KOMMENTAR EG-RICHTLINIE PRODUKTHAFTUNG [1 COMMENTARY EC DIRECTIVE PRODUCT LIABILITY] art. 6 recital 144 (1986) (with further references); HANNS FITZ ET AL, PRODUKTHAFTUNG [PRODUCT LIABILITY] § 5 recital 70 (2004).

[1671] *Cf.* Product Liability Directive art. 6(1)(b).

5.3.3.4. Defenses Allowed to Producers

To succeed in a product liability action, the plaintiff has to prove that the product was defective, that he suffered damages, and that there is a causal relationship between defect and damage.[1672]

The producer cannot be held liable, however, if he proves one of the following: First he may prove that he is indeed not to be treated as a producer because he has not put the product into circulation.[1673]

Second, the producer may prove that the product was neither manufactured for distribution for economic purposes nor manufactured or distributed by him in the course of his business.[1674] This defense is of great significance for non-commercial software manufacturers because they too are producers under Product Liability Directive article 3(1).[1675] If a producer can prove that he develops and distributes software in his private capacity (i.e. not in the course of his business) and not for economic purposes, he cannot be held liable under the Directive. This typically exempts software developers that—like the author[1676]—develop or contribute to open source software in their free time. However, this defense is not available to open source

[1672] *See* Product Liability Directive art. 4.

[1673] *See* Product Liability Directive art. 7(a). *Cf.* HANS CLAUDIUS TASCHNER & EDWIN FRIETSCH, PRODUKTHAFTUNGSGESETZ UND EG- PRODUKTHAFTUNGSRICHTLINIE [PRODUCT LIABILITY ACT AND EC PRODUCT LIABILITY DIRECTIVE] 187 (2d ed. 1990) (naming the theft of and subsequent sale of a previously uncirculated product as an example).

[1674] *See* Product Liability Directive art. 7(c). HANS CLAUDIUS TASCHNER & EDWIN FRIETSCH, PRODUKTHAFTUNGSGESETZ UND EG- PRODUKTHAFTUNGSRICHTLINIE [PRODUCT LIABILITY ACT AND EC PRODUCT LIABILITY DIRECTIVE] 191 (2d ed. 1990)

[1675] *Cf. supra* chapter 5.3.3.2.

[1676] *See, e.g.,* http://pear.php.net/package/XML_Query2XML (last accessed Feb. 10, 2011).

software manufacturers that use open source as a business model (e.g. to attract customers to other commercial products or services).[1677]

Third, the producer may prove that "it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him."[1678] This may be relevant to a software manufacturer if he allows distributers to customize the software. For example, manufacturers of operating system software often allow so-called value-added resellers (VARs)[1679] to sell computers with the operating system pre-installed and configured to meet the VARs' customers' needs. If the operating system manufacturer is able to prove that the vulnerability in question was introduced by the VAR (i.e. did not exist at the time he put the operating system into circulation), he would avoid liability. Furthermore, this defense may be available for software updates: If one of the updates has a defect, the manufacturer could claim that the update (which is typically not distributed on a tangible medium) was not a product[1680] and the original software itself—which may have been distributed on a tangible medium—did not contain the defect when it was put into circulation.

[1677] *Cf.* HENRY CHESBROUGH, OPEN BUSINESS MODELS: HOW TO THRIVE IN THE NEW INNOVATION LANDSCAPE 45 (2006) (describing various open source business models). Examples of companies that have built business models on open source (and could therefore not claim to be exempt from product liability) are Red Hat, Inc., MySQL AB (acquired by Sun Microsystems in Feb. 2008 which was in turn acquired by Oracle, Inc. in Jan. 2010), and IBM.

[1678] Product Liability Directive art. 7(b).

[1679] Often also referred to as original equipment manufacturers (OEMs). *Cf.* GENE K. LANDY & AMY J. MASTORBATTISTA, THE IT / DIGITAL LEGAL COMPANION: A COMPREHENSIVE BUSINESS GUIDE TO SOFTWARE, IT, INTERNET, MEDIA AND IP LAW 379 (2008).

[1680] Furthermore, if the updates are only provided on a subscription-based model—as is typically the case for commercial anti-malware software—the software manufacturer might argue that the updates are not products but are part of a service. For an example of a damaging anti-malware software update see Mark Hofman, *AVG Update Bricking windows 7 64 bit*, SANS INTERNET STORM CENTER, Dec. 3, 2010, http://isc.sans.edu/diary.html?storyid=10030.

Fourth, the producer may prove that "the defect is due to compliance of the product with mandatory regulations issued by the public authorities."[1681] This defense may only be possible where regulation demands the implementation of certain standards or features that contain inherent vulnerabilities.[1682] Voluntary standards and guidelines as developed by ISO or by non-regulatory agencies such as NIST or ENISA are, however, not "mandatory regulations."[1683] Compliance with such standards and guidelines therefore constitutes no defense against a product liability claim.

Fifth, the manufacturer may prove that "the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered."[1684] In particular, this may be relevant if the software in question uses a cryptographic algorithm that was thought to be "secure" but was later discovered to be breakable.[1685]

[1681] *See* Product Liability Directive art. 7(d).

[1682] For example, if a regulation, prior to Nov. 2009, had required software to be fully compliant with the Transport Layer Security (TLS) Protocol, version 1.2 as specified in RFC 5246, that software would have had a vulnerability that was directly caused by a flaw in the design of TLS (CVE-2009-3555). To fix this flaw, RFC 5246 had to be updated. *See* E. RESCORLA, TRANSPORT LAYER SECURITY (TLS) RENEGOTIATION INDICATION EXTENSION, RFC 5746 (2010), ftp://ftp.rfc-editor.org/in-notes/rfc5746.txt. *Cf. also* DIERKS & E. RESCORLA, THE TRANSPORT LAYER SECURITY (TLS) PROTOCOL VERSION 1.2, RFC 5246 (2008), ftp://ftp.rfc-editor.org/in-notes/rfc5246.txt.

[1683] *See* HANS CLAUDIUS TASCHNER & EDWIN FRIETSCH, PRODUKTHAFTUNGSGESETZ UND EG-PRODUKTHAFTUNGSRICHTLINIE [PRODUCT LIABILITY ACT AND EC PRODUCT LIABILITY DIRECTIVE] 194 (2d ed. 1990); HANS JOSEF KULLMANN, PRODUKTHAFTUNGSGESETZ [PRODUCT LIABILITY ACT] 56 (3d ed. 2001).

[1684] *See* Product Liability Directive art. 7(e). *Cf.* Case C-300/95, Comm'n v. United Kingdom, 1997 E.C.R. I-02649, §§ 26-29 (holding that the state of scientific and technical knowledge is an objective one and includes "the most advanced level of such knowledge, without any restriction as to the industrial sector concerned" but is limited to knowledge that has "been accessible at the time when the product in question was put into circulation"). Note that, pursuant to Product Liability Directive art. 15(1)(b), Member States may choose not to implement art. 7(e). Only Finland and Luxembourg have chosen to make use of this option. *See Third Commission report on the application of Council Directive 85/374/EEC*, at 10, COM (2006) 496 final (Sept. 14, 2006).

[1685] For example, the cryptographic hash function MD5 was thought to be very secure in the sense that it was deemed highly unlikely that two MD5 hashes calculated from different data would be identical. However, since

Sixth, if the manufacturer only produced a component of the product in question, he may prove that "the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product."[1686] This defense may be available to software manufacturers who were contracted by another software manufacturer to only develop certain parts of the software product.

5.3.3.5. Recoverable Damages

Article 9 of the Product Liability Directive defines "damage" with reference to two categories of damages: (1) "damage caused by death or by personal injuries"[1687] and (2) "damage to, or destruction of, any item of property other than the defective product itself."[1688]

The second category is further limited in two ways: First, it provides a "lower threshold" of €500. This not only means that property damages below €500 cannot be recovered;[1689] it also

2004 a number of serious flaws were discovered in MD5 leading US-CERT to conclude that "[MD5] should be considered cryptographically broken and unsuitable for further use." *See* US-CERT, MD5 vulnerable to collision attacks, Vulnerability Note VU#836068 (Dec. 31, 2008), http://www.kb.cert.org/vuls/id/836068. *Cf.* XIAOYUN WANG ET AL., COLLISIONS FOR HASH FUNCTIONS MD4, MD5, HAVAL-128 AND RIPEMD (2004), *available at* http://eprint.iacr.org/2004/199.pdf; JOHN BLACK ET AL., A STUDY OF THE MD5 ATTACKS: INSIGHTS AND IMPROVEMENTS (2006), *available at* http://www.cs.colorado.edu/~jrblack/papers/md5e-full.pdf; MARC STEVENS ET AL., VULNERABILITY OF SOFTWARE INTEGRITY AND CODE SIGNING APPLICATIONS TO CHOSEN-PREFIX COLLISIONS FOR MD5 (2007), *available at* http://www.win.tue.nl/hashclash/SoftIntCodeSign/; MARC STEVENS ET AL., CHOSEN-PREFIX COLLISIONS FOR MD5 AND APPLICATIONS (2009), *available at* https://documents.epfl.ch/users/l/le/lenstra/public/papers/lat.pdf.

[1686] *See* Product Liability Directive art. 7(f).

[1687] Product Liability Directive art. 9(a).

[1688] Product Liability Directive art. 9(b).

[1689] *See* Case C-52/00, Comm'n v. France, 2002 E.C.R. I-3827, §§ 26-35 and Case C-154/00, Comm'n v. Greece, 2002 E.C.R. I-03879, § 34 (holding that allowing the recovery of damages of less than €500 violates Product Liability Directive art. 9(b)); *Cf. also* Case C-203/99, Henning Veedfald v. Århus Amtskommune, 2001 E.C.R. I-03569, § 26.

reduces, for those damages that exceed €500, the recoverable amount by €500.[1690] The stated rationale for this threshold is "to avoid litigation in an excessive number of cases."[1691]

Second, damages to any item of property are only recoverable if the item of property (1) "is of a type ordinarily intended for private use or consumption,"[1692] and (2) "was used by the injured person mainly for his own private use or consumption."[1693] These cumulative requirements make clear that, ultimately, the Product Liability Directive is a consumer protection measure.[1694]

Concerning the issue of immaterial damages which may arise with regard to both categories of damages, article 9 of the Product Liability Directive leaves it to the Member States to decide whether to allow for their recovery.[1695]

[1690] *See* Product Liability Directive recital 9 (stating that "compensation for damage to property; whereas the latter should […] be subject to a *deduction of a lower threshold* of a fixed amount" (emphasis added)). The German and French language versions of art. 9(b) are more explicit and refer to "Selbstbeteiligung" and "sous déduction d'une franchise" respectively. *See* JOACHIM SCHMIDT-SALZER, 1 KOMMENTAR EG-RICHTLINIE PRODUKTHAFTUNG [1 COMMENTARY EC DIRECTIVE PRODUCT LIABILITY] art. 9 recital 58 (1986); HANS CLAUDIUS TASCHNER & EDWIN FRIETSCH, PRODUKTHAFTUNGSGESETZ UND EG- PRODUKTHAFTUNGSRICHTLINIE [PRODUCT LIABILITY ACT AND EC PRODUCT LIABILITY DIRECTIVE] 383 (2d ed. 1990); HANS JOSEF KULLMANN, PRODUKTHAFTUNGSGESETZ 170 (3d ed. 2001). Note that the Commission chose not to bring actions against Member States that made the full amount of damages recoverable if it exceeds €500. *See Third Commission report on the application of Council Directive 85/374/EEC*, at 11, COM (2006) 496 final (Sept. 14, 2006).

[1691] Product Liability Directive recital 9.

[1692] Product Liability Directive art. 9(b)(i).

[1693] Product Liability Directive art. 9(b)(ii).

[1694] *Cf.* Product Liability Directive recitals 1, 4-6, 8, 9, 12, 13, 15-17, and 19 (all referring to the "protection of the consumer"). Note, however, that the Directive does not preclude Member States from making producers liable for damages to items of property that are intended or employed for professional use. *See* Case C-285/08, Moteurs Leroy Somer v. Dalkia France, 2009 ECR I-04733, §§ 30-31 (holding that since the Product Liability Directive does not cover compensation for damage to an item of property intended for professional use and employed for that purpose, Member States are free to make producers liable for such damages under a system of liability which corresponds to that established by the Directive).

[1695] *See* Product Liability Directive art. 9 (stating that "[t]his Article shall be without prejudice to national provisions relating to non-material damage"). *See also id.* recital 9 (stating that the Directive "should not prejudice compensation for pain and suffering and other non-material damages payable, where appropriate, under the law applicable to the case"). *Cf.* CHRISTOPH ANDERLE, DER HAFTUNGSUMFANG DES HARMONISIERTEN PRODUKTHAFTUNGSRECHTES [THE EXTENT OF LIABILITY UNDER HARMONIZED PRODUCT LIABILITY LAW] 67

The Product Liability Directive requires Member States to provide for the compensation for economic losses which are suffered as a result of death or personal injuries[1696] but not when they are the result of property damages.[1697] Purely economic losses that are directly caused by a product defect—and not by death, personal injury, or property damage—are also not covered by the Product Liability Directive.[1698]

Furthermore, the Directive provides two ways in which Member States may limit or reduce a producer's liability. First, article 8(2) allows Member States to reduce or disallow a producer's liability when, "having regard to all the circumstances, the damage is caused both by a defect in the product and by the fault of the injured person or any person for whom the

(1990); Hans Claudius Taschner & Edwin Frietsch, Produkthaftungsgesetz und EG-Produkthaftungsrichtlinie [Product Liability Act and EC Product Liability Directive] 384 (2d ed. 1990). For a brief overview of the legal situation in the different Member States see Lovells, Product liability in the European Union: A report for the European Commission 21 (2003), *available at* http://ec.europa.eu/enterprise/policies/single-market-goods/files/goods/docs/liability/studies/lovells-study_ en.pdf.

[1696] *See* Product Liability Directive art. 9(a) (referring to "damage *caused by* death or by personal injuries" (emphasis added)). *Cf.* Joachim Schmidt-Salzer, 1 Kommentar EG-Richtlinie Produkthaftung [1 Commentary EC Directive Product Liability] art. 9 recital 14 et seq. (1986). Hans Claudius Taschner & Edwin Frietsch, Produkthaftungsgesetz und EG- Produkthaftungsrichtlinie [Product Liability Act and EC Product Liability Directive] 380 (2d ed. 1990).

[1697] Product Liability Directive art. 9(b)—unlike art. 9(a)—does not refer to "damage caused by" but to "*damage to* any item of property" (emphasis added). *See* Hans Claudius Taschner & Edwin Frietsch, Produkthaftungsgesetz und EG- Produkthaftungsrichtlinie [Product Liability Act and EC Product Liability Directive] 386 (2d ed. 1990) (arguing that such economic losses are not covered by the Directive and only recoverable in a contractual relationship); Hermann Hollmann, *Die EG-Produkthaftungsrichtlinie* [*The EC Product Liability Directive*], 1985 Der Betrieb 2439 (F.R.G.). *But see* Joachim Schmidt-Salzer, 1 Kommentar EG-Richtlinie Produkthaftung [1 Commentary EC Directive Product Liability] art. 9 recital 29 et seq. (1986) (arguing economic losses due to property damage are covered because (1) insurance was available for economic losses due to property damage, (2) the different wording in art. 9(b) was only meant to clarify that damages to the defective product itself are not recoverable, and (3) a single liability regime would be more practicable).

[1698] Product Liability Directive art. 9 makes no reference to pure economic losses. *See* Joachim Schmidt-Salzer, 1 Kommentar EG-Richtlinie Produkthaftung [1 Commentary EC Directive Product Liability] art. 9 recital 36 (1986); Hans Claudius Taschner & Edwin Frietsch, Produkthaftungsgesetz und EG- Produkthaftungsrichtlinie [Product Liability Act and EC Product Liability Directive] 384 (2d ed. 1990).

injured person is responsible."[1699] For example, if damages are cause by a worm[1700] that exploited a software defect but could have been prevented from spreading by keeping anti-malware software current, it could be argued that the failure to regularly update the anti-malware software constituted a fault, based on which Member States are allowed to reduce or disallow liability.

Second, article 16(1) of the Product Liability Directive allows Member States to limit a producer's total liability for damage resulting from death or personal injury and caused by the same product defect.[1701] If a Member State chooses to introduce such a liability cap, it has to be at least €70 million.[1702] It should be noted that the Directive does not provide for a liability cap for property damages.[1703]

In summary, the rather complicated but ultimately narrow definition of recoverable damages significantly reduces the extent to which the Product Liability Directive can be used as an instrument to hold software manufacturers accountable. Not only are damages suffered by professional users not recoverable; liability is also limited to property damages and damages

[1699] Product Liability Directive art. 8(2). Note, however, that liability cannot be reduced if the damage is caused by a product defect and by "the act or omission of a third party." *See id.* art. 8(1).

[1700] *See* chapter 3.1 (discussing technological threats such as worms).

[1701] *See* Product Liability Directive art. 16(1).

[1702] *See id. Cf.* Product Liability Directive recital 17 (stating that a liability cap established by a Member State has to be "sufficiently high to guarantee adequate protection of the consumer and the correct functioning of the common market").

[1703] As Product Liability Directive recital 17 explains, the possibility of a liability cap was a concession to Member States that had a tradition of limited liability for damages resulting from a death or personal injury. *Cf.* JOACHIM SCHMIDT-SALZER, 1 KOMMENTAR EG-RICHTLINIE PRODUKTHAFTUNG [1 COMMENTARY EC DIRECTIVE PRODUCT LIABILITY] art. 16 recital 12 (1986).

caused by death or personal injuries, thereby excluding purely economic losses which constitute the vast majority of damages caused by software defects.[1704]

5.3.4. Seller Liability Under the EU Consumer Sales Directive

Parliament and Council Directive 1999/44[1705] (hereinafter *Consumer Sales Directive*) harmonizes certain aspects of the sale of consumer goods and associated guarantees.

Besides introducing rules for voluntary guarantees—which will be discussed in chapter 5.3.4.4—the Consumer Sales Directive provides in article 2 an obligation for the seller of consumer goods to deliver goods that are "in conformity with the contract of sale"[1706] and further defines certain remedies available to a consumer.[1707] Neither the obligation itself nor the available remedies can be derogated from to the consumer's disadvantage by contractual means.[1708]

It is important to emphasize that liability under article 2 of the Consumer Sales Directive only applies to sellers but not producers. However, since software manufacturers are significantly

[1704] *Cf.* Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 302 (2006) (discussing various types of economic losses typically suffered due to software system security breaches).

[1705] 1999 O.J. (L 171) 12 (EC).

[1706] EU Consumer Goods Directive art. 2(1).

[1707] *See infra* chapter 5.3.4.3.

[1708] *See* Consumer Sales Directive art. 7(1) (stating that "[a]ny contractual terms or agreements concluded with the seller before the lack of conformity is brought to the seller's attention which directly or indirectly waive or restrict the rights resulting from this Directive shall, as provided for by national law, not be binding on the consumer"). *Cf.* TILMAN REPGEN, KEIN ABSCHIED VON DER PRIVATAUTONOMIE: DIE FUNKTION ZWINGENDEN RECHTS IN DER VERBRAUCHSGÜTERKAUFRICHTLINIE [NO FAREWELL TO PRIVATE AUTONOMY: THE ROLE OF *IUS COGENS* IN THE CONSUMER SALES DIRECTIVE] 98 et seq. (2001) (discussing why the fact that the Consumer Sales Directive requires Member States to implement its provisions as *ius cogens* does not reduce but indeed strengthens private autonomy).

more important actors in the information security landscape than software retailers,[1709] this chapter discusses liability under article 2 of the Consumer Sales Directive in the context of software manufacturers which may come in the scope of article 2 if they can be said to have directly sold software to a consumer.

With regard to cases where the consumer buys software from a retailer rather than the software manufacturer, it is only noted that Consumer Sales Directive article 4 refers to the possibility that the final seller—should he be held liable by a consumer—might have a right of redress under national law against the previous seller in the same chain of contracts (or any other intermediary) which may be the software manufacturer.[1710] However, under the Directive, any such national law can be derogated from by contractual means.[1711] Since large software manufacturers (e.g. Adobe, Apple, or Microsoft) are typically in a stronger bargaining position than retailers,[1712] they are able to avoid any liability to their retailers.

[1709] In contrast to software manufacturers, software retailers typically have, technically speaking, no capability to improve the level of security of a software they sell. *Cf. supra* chapter 2.3.3 (discussing the role of software manufacturers).

[1710] *See* Consumer Sales Directive art. 4. Since this provision of the Directive is not strictly consumer protection related, it has been the subject of much debate. For an overview of the current state of the debate see THOMAS ZERRES, DIE BEDEUTUNG DER VERBRAUCHSGÜTERKAUFRICHTLINIE FÜR DIE EUROPÄISIERUNG DES VERTRAGSRECHTS [THE SIGNIFICANCE OF THE CONSUMER SALES DIRECTIVE FOR THE EUROPEANIZATION OF CONTRACT LAW] 425 (2007); ROBERT BRADGATE & CHRISTIAN TWIGG-FLESNER, CONSUMER SALES AND ASSOCIATED GUARANTEES 228 (2003).

[1711] *See* Consumer Sales Directive recital 9 (stating that "the seller should be free, as provided for by national law, to pursue remedies against the producer, a previous seller in the same chain of contracts or any other intermediary, *unless he has renounced that entitlement*" (emphasis added)). *Cf.* THOMAS ZERRES, DIE BEDEUTUNG DER VERBRAUCHSGÜTERKAUFRICHTLINIE FÜR DIE EUROPÄISIERUNG DES VERTRAGSRECHTS [THE SIGNIFICANCE OF THE CONSUMER SALES DIRECTIVE FOR THE EUROPEANIZATION OF CONTRACT LAW] 429 (2007) (with further references). For a critical perspective see MICHAEL HASSEMER, HETERONOMIE UND RELATIVITÄT IN SCHULDVERHÄLTNISSEN [HETERONOMY AND RELATIVITY IN OBLIGATIONS] 127 (2007).

[1712] Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283 (2006).

The following chapters will discuss the software manufacturer's liability as a seller with regard to the liability's scope of application, the issue of contract conformity, as well as the available remedies.

5.3.4.1. Scope of Application

Consumer Sales Directive article 2 only applies if there is a "sale" of "consumer goods" between a "seller"[1713] and a "consumer."[1714]

The most significant element, determining the extent to which software manufacturers can be held liable under article 2 is that of "consumer goods." This term is defined as "any *tangible* movable item […]."[1715] This makes clear that software, when downloaded over the Internet, is not a "consumer good."[1716] If software is distributed on a CD or another tangible medium, its status as a consumer good is—similar to its status as a "product" under the Product Liability Directive[1717]—affirmed by some commentators[1718] but still controversial.[1719] If software is

[1713] Consumer Sales Directive art. 1(2)(c) (defining "seller" as "any natural or legal person who, under a contract, sells consumer goods in the course of his trade, business or profession").

[1714] Consumer Sales Directive art. 1(2)(a) (defining "consumer" as "any natural person who, in the contracts covered by this Directive, is acting for purposes which are not related to his trade, business or profession").

[1715] Consumer Sales Directive art. 1(2)(b) (emphasis added). Not relevant here but exempted from this definition are: goods sold by way of execution or otherwise by authority of law, water and gas where they are not put up for sale in a limited volume or set quantity, and electricity.

[1716] *See* Augustín Luna Serrano, *in* EU KAUFRECHTS-RICHTLINIE [EU SALES LAW DIRECTIVE] art. 1 recital 33 (Stefan Grundmann & Cesare Massimo Bianca eds., 2002). *See also Commission Green Paper on the Review of the Consumer Acquis*, at 12, COM (2006) 744 final (Feb. 8, 2007) (discussing the "possible extension of the [EU Consumer Sale Directive's] scope in order to include intangible goods, such as software and data"); European Parliament resolution of 6 September 2007 on the Green Paper on the Review of the Consumer Acquis, A6-0281/2007, § 31 (stating that it "[c]onsiders that it is appropriate to examine issues relating to the protection of consumers when they conclude contracts providing digital content, software and data, in the light of the protection afforded by Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees; asks the Commission to examine this matter in detail so *as to determine whether it is appropriate to propose one or more specific rules or to extend the rules* set out in that Directive to this type of contract" (emphasis added)).

[1717] *See supra* chapter 5.3.3.1.

integrated into an electronic device, however, it is generally considered part of a consumer good.[1720]

Since many applications are being migrated to the web—i.e. implemented as online services rather than software that can be installed and run on a user's computer[1721]—it has to be emphasized that services are not covered by the Consumer Sales Directive.[1722]

Another issue that challenges the application of Consumer Sales Directive article 2 on software is that it only covers "sales."[1723] Software is, however, typically not sold but licensed.[1724]

The Consumer Sales Directive does not define the term "sale"; it does, however, provide that "[c]ontracts for the supply of consumer goods to be manufactured or produced" are also contracts of sale for the purpose of the Directive, suggesting a more flexible understanding of

[1718] *Cf.* Augustín Luna Serrano, *in* EU KAUFRECHTS-RICHTLINIE [EU SALES LAW DIRECTIVE] art. 1 recital 33 n.2 (Stefan Grundmann & Cesare Massimo Bianca eds., 2002).

[1719] *Cf.* ROBERT BRADGATE & CHRISTIAN TWIGG-FLESNER, CONSUMER SALES AND ASSOCIATED GUARANTEES 22 (2003).

[1720] *Cf. supra* chapter 5.3.3.1 for a discussion of the same issue in the context of the Product Liability Directive.

[1721] *Cf.* chapter 2.3.3 (discussing cloud computing and application service providing). Examples include Windows Live Hotmail, Google Docs, and Facebook.

[1722] *Cf. Commission Proposal for a European Parliament and Council Directive on the sale of consumer goods and associated guarantees*, at 11, COM (1995) 520 final (June 18, 1996) (stating that "the Commission considers that the complexity and diversity of services do not lend themselves to a simple extension to services of rules governing the sale of goods").

[1723] *Cf.* Consumer Sales Directive art. 2(1).

[1724] This became apparent in the recent decision of Vernor v. Autodesk, Inc., 621 F.3d 1102, 1111 (9th Cir. 2010) ("a software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions"; as a licensee, Vernor was not entitled to invoke the first sale doctrine). *Cf. also* Bundesgerichtshof [BGH] [Federal Court of Justice] Feb. 3, 2011, I ZR 129/08 (F.R.G.) (making a referral for a preliminary ruling to the ECJ regarding the question of whether a user who has purchased a "used" software has the right to run the software—and thereby copy it into the computer's memory—under Parliament and Council Directive 2009/24, art. 5(1), 2009 O.J. (L 111) 16, 18 (EC) which grants a "lawful acquirer" the right to use software "in accordance with its intended purpose").

the term "sale." It has therefore been suggested in the literature that software licenses that are more similar to contracts of sale than contracts of lease should be treated as "sales" under the Consumer Sales Directive.[1725] However, until the ECJ rules on the issue, significant uncertainty remains as to whether the commercial licensing of software constitutes a sale.

What is clear, however, is that even if commercial software licenses can be considered a sale, free software licenses cannot. This is important because, today, a significant amount of software is given away for free. This does not only include open source software which is typically freely available but also closed software that is given away to increase the switching costs and network effects for customers of a related product[1726] or to further other commercial objectives.[1727]

However, software for which a licensee does not have to pay money for but for which he has to grant the licensor certain intellectual property rights or the right to process the licensee's personal information is not "free."[1728] Accordingly, such software licenses should be treated the same as licenses for which the licensee has to pay a monetary fee.

[1725] Augustín Luna Serrano, *in* EU KAUFRECHTS-RICHTLINIE [EU SALES LAW DIRECTIVE] art. 1 recital 33 (Stefan Grundmann & Cesare Massimo Bianca eds., 2002) (referring to GIOVANNI DE CRISTOFARO, DIFETTO DI CONFORMITÀ AL CONTRATTO E DIRITTI DEL CONSUMATORE. L'ORDINAMENTO ITALIANO E LA DIRETTIVA 99/44/CE SULLA VENDITA E LE GARANZIE DEI BENI DI CONSUMO [LACK OF CONFORMITY WITH THE CONTRACT AND CONSUMER RIGHTS. THE ITALIAN SYSTEM AND DIRECTIVE 99/44/EC ON THE SALE OF CONSUMER GOODS AND ASSOCIATED GUARANTEES] 42 et seq. (2000)).

[1726] Examples include Adobe Flash Player and Adobe Reader (formerly Acrobat Reader) which are given away for free to increase the value of Adobe software that can be used to create Flash and Acrobat content respectively. Switching costs and network effects are briefly discussed *supra* in chapter 2.3.3.

[1727] For example for advertisement purposes.

[1728] For example, until Sept. 2008, the license terms of Google Chrome stated: "By submitting, posting or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any content which you submit, post or display on or through, the services." *See* Ina Fried, *Be sure to read Chrome's fine print*, CNET.COM, Sept. 2, 2008, http://news.cnet.com/8301-13860_3-10030522-56.html?tag=mncol;txt.

5.3.4.2. Conformity with the Contract

Article 2(1) of the Consumer Sales Directive provides that the goods that are delivered by the seller have to be, at the time of delivery,[1729] "in conformity with the contract of sale."[1730] Article 2(2) further provides a number of cumulative[1731] conditions under which a rebuttable presumption of conformity with the contract is created. The first two are of a subjective nature and can be characterized as implied contract terms while the third and fourth are of a more objective nature[1732]:

First, the goods have to "comply with the description given by the seller" and have to "possess the qualities of the goods which the seller has held out to the consumer as a sample or model."[1733]

Second, they have to be "fit for any particular purpose for which the consumer requires them and which he made known to the seller at the time of conclusion of the contract and which the seller has accepted."[1734]

[1729] *Cf.* Consumer Sales Directive art. 3(1) (making clear that the seller is liable to the consumer only for any lack of conformity "which exists at the time the goods were delivered.").

[1730] Consumer Sales Directive art. 2(1).

[1731] *See* Consumer Sales Directive recital 8 (stating that "the elements mentioned in the presumption are cumulative; whereas, if the circumstances of the case render any particular element manifestly inappropriate, the remaining elements of the presumption nevertheless still apply"). *Cf.* THOMAS ZERRES, DIE BEDEUTUNG DER VERBRAUCHSGÜTERKAUFRICHTLINIE FÜR DIE EUROPÄISIERUNG DES VERTRAGSRECHTS [THE SIGNIFICANCE OF THE CONSUMER SALES DIRECTIVE FOR THE EUROPEANIZATION OF CONTRACT LAW] 54 (2007); Stefan Grundmann, *in* EU KAUFRECHTS-RICHTLINIE [EU SALES LAW DIRECTIVE] art. 2 recital 19 (Stefan Grundmann & Cesare Massimo Bianca eds., 2002); SIBYLLE HÖFFE, DIE VERBRAUCHSGÜTERKAUFRICHTLINIE 1999/44/EG UND IHRE AUSWIRKUNGEN AUF DEN SCHADENSERSATZ BEIM KAUF [THE CONSUMER SALES DIRECTIVE 1999/44/EC AND ITS EFFECTS ON SALES CONTRACT LIABILITY] 27 (2002).

[1732] *Cf.* Stefan Grundmann, *in* EU KAUFRECHTS-RICHTLINIE [EU SALES LAW DIRECTIVE] art. 2 recital 8 (Stefan Grundmann & Cesare Massimo Bianca eds., 2002).

[1733] Consumer Sales Directive art. 2(2)(a).

[1734] Consumer Sales Directive art. 2(2)(b).

Third, the goods have to be fit "for the purposes for which goods of the same type are normally used."[1735] This is a truly objective standard that significantly broadens what is required for a good to be conformant with the contract.[1736] However, as further discussed *infra*, a consumer will not be able to rely on this requirement if he "could not reasonably [have been] unaware"[1737] that the good was not fit for its normal purpose.

Fourth, the goods have to "show the quality and performance which are normal in goods of the same type and which the consumer can reasonably expect."[1738] These reasonable expectations are based on "the nature of the goods" and "any public statements on the specific characteristics of the goods made about them by the seller, the producer or his representative, particularly in advertising or on labelling."[1739] The reference to the "nature of the goods" is to be seen as complementary to the third condition discussed *supra*.[1740] The reference to public statements made by the seller or the producer is particularly significant because advertisement largely shapes consumer expectations. For example, if a software manufacturer advertises his software as not requiring users "to deal with viruses, malware and security updates,"[1741] to

[1735] Consumer Sales Directive art. 2(2)(c).

[1736] ROBERT BRADGATE & CHRISTIAN TWIGG-FLESNER, CONSUMER SALES AND ASSOCIATED GUARANTEES 59 (2003); Stefan Grundmann, *in* EU KAUFRECHTS-RICHTLINIE [EU SALES LAW DIRECTIVE] art. 2 recital 26 (Stefan Grundmann & Cesare Massimo Bianca eds., 2002).

[1737] *Cf.* Consumer Sales Directive art. 2(3).

[1738] Consumer Sales Directive art. 2(2)(d).

[1739] *Id.*

[1740] A distinction between the third condition and this aspect of the fourth condition is not practically relevant. *Cf.* Stefan Grundmann, *in* EU KAUFRECHTS-RICHTLINIE [EU SALES LAW DIRECTIVE] art. 2 recital 26 (Stefan Grundmann & Cesare Massimo Bianca eds., 2002). Contrary to what recital 8 of the Directive suggests, it is irrelevant with regard to software whether it is "new" or "second-hand." *Cf.* Consumer Sales Directive recital 8 (stating that "the quality and performance which consumers can reasonably expect will depend inter alia on whether the goods are new or second-hand").

[1741] Sundar Pichai, Vice President, Google Inc., *Introducing the Google Chrome OS*, OFFICIAL GOOGLE BLOG, July 7, 2009, http://googleblog.blogspot.com/2009/07/introducing-google-chrome-os.html. *Cf.* Grant Gross, have been designed to be "highly secure from day one"[1742] or even to be "unbreakable,"[1743] considerably higher levels of security will be required from the software to be "in conformity with the contract." However, the seller is not bound by public statements made by him or the producer if he shows that (a) he was not, and could not reasonably have been, aware of the statement in question, (b) by the time of conclusion of the contract the statement had been corrected, or (c) the decision to buy the consumer goods could not have been influenced by the statement.[1744]

As previously noted, the fulfillment of these four cumulative conditions only creates the rebuttable presumption of compliance with the contract. The non-fulfillment of one of the conditions does not, however, create a presumption of non-compliance.

Furthermore, the relatively strong position for consumers brought about by the difficulty of creating the above presumption is put into perspective by article 2(3) of the Consumer Sales Directive which provides that a good *is in conformity* with the contract "if at the time the contract was concluded," the consumer (1) was aware, or (2) could not reasonably be unaware of, the lack of conformity,[1745] or (3) if the lack of conformity has its origin in materials

Google's OS Security Claims Called 'idiotic', PCWORLD, July 8, 2009, http://www.pcworld.com/businesscenter/article/168087/googles_os_security_claims_called_idiotic.html (quoting Bruce Schneier).

[1742] http://www.apple.com/safari/what-is.html (last accessed Feb. 10, 2011).

[1743] In 2002, Oracle advertised its relational database management system Oracle9i with the slogan "Unbreakable. Can't break it. Can't break in." *See* Kevin Poulsen, *Breakable*, SECURITYFOCUS, Jan. 16, 2002, http://www.securityfocus.com/news/309. Note that it is unlikely but not unthinkable that Oracle9i would be used by consumers.

[1744] Consumer Sales Directive art. 2(4).

[1745] *Cf. Commission Proposal for a European Parliament and Council Directive on the sale of consumer goods and associated guarantees*, at 12, COM (1995) 520 final (June 18, 1996) (equating situations in which the consumer "could not have been unaware of the lack of conformity at the time of purchase" with "patent defect present in the good which the consumer has examined prior to purchase").

supplied by the consumer.[1746] Cases (1) and (2) can become an issue particularly in the context of the third and fourth condition discussed *supra*, that is if a reasonable consumer would have (or the consumer in question did) know that the software was not “fit for the purposes for which goods of the same type are normally used”[1747] or did not “show the quality and performance” which can be reasonably expected “taking into account any public statements [made] by the seller [or] the producer.”[1748] Case (3) is close to irrelevant with regard to software because indeed very few consumers have custom software built according to their specifications or with the inclusion of their own code—both of which would have to be regarded as “materials supplied by the consumer.”[1749]

With regard to the security of software, the fundamental question is therefore: Is software that contains security vulnerabilities generally in conformity with the contract? Since software vulnerabilities are regularly discussed in the media, consumers “could not reasonably be unaware of”[1750] the fact that all commercial off-the-shelf software contains vulnerabilities—no more than they are “entitled to expect” vulnerability-free software products under the Product Liability Directive.[1751] Accordingly, the fact that a software is not vulnerability-free does not constitute a lack of conformity with the contract—unless the seller promised that the software would be vulnerability-free.[1752] What is then, the level of security, a consumer can

[1746] Consumer Sales Directive art. 2(3).

[1747] *Cf.* Consumer Sales Directive art. 2(2)(c).

[1748] *Cf.* Consumer Sales Directive art. 2(2)(d).

[1749] *Cf.* Consumer Sales Directive art. 2(3).

[1750] *Id.*

[1751] *See supra* chapter 5.3.3.3.

[1752] *Cf.* Consumer Sales Directive art. 2(1).

"reasonably expect" and what is the lowest level of software security, a consumer could "not reasonably be unaware of"?

While most security vulnerabilities have to be expected, some, through a combination of their severity and ease with which they could have been prevented, are not to be expected.[1753] However, this only covers a very narrow range of vulnerabilities such as backdoors.[1754] The presence of the vast majority of vulnerabilities therefore does not lead to a lack of conformity with the contract.

Another issue which has also been discussed *supra* in the context of the Product Liability Directive[1755] is that of ineffective security software. If a firewall software does not block network traffic it was configured to block or if backup software does not back up the files it was supposed to, it will not be difficult for a consumer to establish that the software was not in compliance with the contract.

However, many types of security software rely on continuous updates to effectively safeguard against newly discovered threats (e.g. anti-malware software). If the quality of the updates decreases over time, the overall effectiveness of the security software against new threats will continually be reduced. In this situation, the software manufacturer may argue that the update (which is typically not distributed on a tangible medium) was not a consumer good that has been sold[1756] and the original security software itself—which may have been distributed on a

[1753] *Cf.* chapter 5.3.3.3 (discussing the level of safety a person is "entitled to expect" under the Product Liability Directive).

[1754] *Cf. id.*

[1755] *See supra* chapter 5.3.3.3.

[1756] Furthermore, if the updates are only provided on a subscription-based model—as is typically the case for commercial anti-malware software—the software manufacturer might argue that the updates are not goods but are part of a service.

tangible medium—did not show any lack of conformity with the contract when it was delivered.[1757]

This raises the related question whether software goods generally have to implement an automatic update feature to be in compliance with the contract. Such a feature allows users to choose whether newly available security updates should be installed automatically or whether they want to be at least notified about new security updates so that they can install them manually. Since all major manufacturers of Internet-related software intended for consumers have implemented such a feature,[1758] it could be argued that it is generally required for an Internet-related software (e.g. a browser plug-in or an e-mail client) to achieve "the quality and performance which are normal in goods of the same type and which the consumer can reasonably expect."[1759] Internet-related software that does not have an automatic update feature could therefore not benefit from the presumption of conformity with the contract under article 2(2) of the Consumer Sales Directive.

Lastly, a lack of conformity with the contract may be caused by an incorrect installation of the software. Article 2(5) of the Consumer Sales Directive provides that this constitutes a lack of conformity of the goods if (a) the installation forms part of the contract of sale of the goods and the goods were installed by the seller or under his responsibility, or (b) if the product was intended to be installed by the consumer and is installed incorrectly due to "a shortcoming in

[1757] *Cf. supra* chapter 5.3.3.4 (discussing the same issue in the context of the Product Liability Directive).

[1758] In particular Adobe, Apple, and Microsoft have implemented such a feature for its products. *See* http://www.apple.com/softwareupdate/ (last accessed Feb. 10, 2011); http://blogs.adobe.com/adobereader/2010/04/upcoming_adobe_reader_and_acro.html (last accessed Feb. 10, 2011); http://www.microsoft.com/windows/downloads/windowsupdate/default.mspx (last accessed Feb. 10, 2011).

[1759] Consumer Sales Directive art. 2(2)(d).

the installation instructions."[1760] The first case is rather rare with regard to software but the second case, sometimes also referred to as the "IKEA clause,"[1761] applies itself very well to misleading installation and configuration instructions that result in a misconfiguration of the software that in turn creates a vulnerability.

5.3.4.3. Remedies

If the licensing of a software is regarded as a sale of a consumer good and if that software contains a vulnerability that makes it non-conformant with the contract, the question of remedies arises.

Article 3 of the Consumer Sales Directive provides four remedies which are organized in a two-stage hierarchy. Repair or replace in stage one and a price reduction or a rescission of the contract in stage two:

First, the consumer may require the seller to repair or replace the goods, in either case free of charge.[1762] In the case of software, such a repair or replace would be in the form of a software update that brings the software into conformity with the contract. A consumer may not require a repair or replacement if "this is impossible or disproportionate."[1763] Fixing a security

[1760] Consumer Sales Directive art. 2(5).

[1761] *See, e.g.,* Oliver Brand, *Probleme mit der „IKEA-Klausel"* [*Problems with the "IKEA clause"*], 2003 ZEITSCHRIFT FÜR DAS GESAMTE SCHULDRECHT 96 (F.R.G.); CHRISTIAN KAU, VERTRAUENSSCHUTZMECHANISMEN IM INTERNET, INSBESONDERE IM E-COMMERCE [PROTECTION OF LEGITIMATE EXPECTATION ON THE INTERNET, PARTICULARLY IN E-COMMERCE] 82 (2006) (referring to the German transposition of art. 2(5))

[1762] Consumer Sales Directive art. 3(3). "[F]ree of charge" refers to "the necessary costs incurred to bring the goods into conformity, particularly the cost of postage, labour and materials." *Id.* art. 3(b). *Cf.* Case C‑404/06, Quelle AG v. Bundesverband der Verbraucherzentralen und Verbraucherverbände, 2008 ECR I-2685, § 43 (holding that "[a]rticle 3 of the Directive is to be interpreted as precluding national legislation under which a seller who has sold consumer goods which are not in conformity may require the consumer to pay compensation for the use of those defective goods until their replacement with new goods").

[1763] Consumer Sales Directive art. 3(3).

vulnerability is almost never impossible; it may, however, appear disproportionate when, as the Directive suggests,[1764] only the specific consumer's interest in having the vulnerability closed is considered.

In contrast to traditional consumer goods, the manufacturing of software (and other information goods) has high fixed costs but very low marginal costs.[1765] The same is true for the repair or replacement of software: the costs of producing a software update are very high while the costs of distributing the update over the Internet to a user are essentially $0. The total cost of the first repair of a software good is therefore significantly higher than is commonly the case for consumer goods. On the other hand, all subsequent repairs of the same software issue will essentially not cost anything while for traditional consumer goods, each repair causes additional costs.

This characteristic of software should be taken into account when deciding whether a software manufacturer should be required to develop a security update. Specifically, the fixed costs of producing the update should be regarded as distributed to all customers that will eventually have a right to that update.

In the second stage, the consumer may require an appropriate reduction of the price or, if the lack of conformity is not "minor,"[1766] have the contract rescinded.[1767] These remedies are only

[1764] *Id.* (stating that a remedy is disproportionate if "it imposes costs on the seller which, in comparison with the alternative remedy, are unreasonable, taking into account" (a) the value the goods would have if there were no lack of conformity; (b) the significance of the lack of conformity, and (c) whether the alternative remedy could be completed without significant inconvenience to the consumer).

[1765] *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 3 (1999).

[1766] Consumer Sales Directive art. 3(6).

[1767] *See* Consumer Sales Directive art. 3(5).

available to the consumer if (1) the consumer is entitled to neither repair nor replacement, (2) the seller has not completed the remedy within a reasonable time, or (3) the seller has not completed the remedy without significant inconvenience to the consumer.[1768]

For example, if a software manufacturer refuses to provide a security update for publicly disclosed vulnerabilities that lead to a non-conformity of the contract, a consumer could demand a reduction of the price. At least if the vulnerability is already being exploited "in the wild," the lack of conformity caused by the vulnerability cannot be regarded as "minor," allowing the consumer to alternatively have the contract rescinded.

This two-staged hierarchy of remedies—if fully applied to software vulnerabilities—would force software manufacturers to either issue security updates in a timely fashion or repay (part of) the licensing fee. Either option would effectively lead to a substantial transfer of risks related to software vulnerabilities from consumers to software manufacturers.

5.3.4.4. Time Limits

Article 5 of the Consumer Sales Directive provides that the seller may only be held liable under Article 3 "where the lack of conformity becomes apparent within two years as from delivery of the goods."[1769]

As applied to software, this provision strikes an interesting balance. If consumers are satisfied with a certain version of a software, they are often reluctant to upgrade to a newer version, in particular if—as is typically the case—the upgrade is not free. For example, Windows XP

[1768] *See id.*

[1769] Consumer Sales Directive art. 5(1). Note that with regard to second-hand goods, Member States may provide that the seller and consumer may agree on a shorter time period for the liability of the seller than that set down in art. 5(1), as long as such period is not less than one year. *See id.* art. 7(1).

enjoys strong popularity despite having first been released in 2001—more than nine years ago. Software manufacturers, on the other hand, want consumers to purchase the new versions of their products. One way to strongly increase the consumers' incentive to purchase an upgrade is to refuse to provide anymore security updates. Microsoft, for example, has announced that it will not provide any security updates for Windows XP after August 4, 2014.[1770] Smaller software manufacturers, however, only provide security updates for a much shorter time frame. For example, IDM Computer Solutions, Inc., manufacturer of the source code editor UltraEdit which is popular, *inter alia*, among developers of non-commercial software (i.e. consumers)[1771] only provides security updates for one year as from the date of licensing.[1772] Assuming that the licensing of UltraEdit is considered a sale of goods under the Consumer Sales Directive, IDM Computer Solutions would be forced to extend the duration during which it provides security updates to two years (for vulnerabilities that cause non-conformity with the contract) or would have to face consumer claims for price reduction and contract rescission.[1773]

The Consumer Sales Directive allows Member States to introduce another time limit: Member States may provide that, "in order to benefit from his rights, the consumer must inform the

[1770] *See* http://support.microsoft.com/lifecycle/?LN=en-us&x=14&y=12&C2=1173 (last accessed Feb. 10, 2011) (noting that extended support will end on Aug. 4, 2014).

[1771] *Cf. supra* chapter 5.3.4.1.

[1772] *See* http://www.ultraedit.com/updates/ueupdate.html (last accessed Feb. 10, 2011).

[1773] Note that this example is a hypothetical in the sense that, depending on the national law, a court of a Member State may not have jurisdiction to hear such a case against IDM Computer Solutions, Inc. which is domiciled in Hamilton, Ohio. *See* Council Regulation 44/2001, art. 4(1), 2001 O.J. (L 12) 1, 4 (EC) (stating "[i]f the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall […] be determined by the law of that Member State").

seller of the lack of conformity within a period of two months from the date on which he detected such lack of conformity."[1774]

5.3.5. Liability for a Guarantee under the EU Consumer Sales Directive

The Consumer Sales Directive also prescribes certain rules for guarantees that are given voluntarily and given without extra charge by the seller or the producer.[1775] The primary purpose of these rules is to ensure that guarantees do not mislead the consumer, in particular with regard to the consumer's legal rights under the Directive.[1776]

First, Article 6 of the Consumer Sales Directive provides that guarantees are binding on the offerer "under the conditions laid down in the guarantee statement and the associated advertising."[1777]

Second, a guarantee has to contain certain information so as not to mislead the consumer.[1778] It has to (1) state that the consumer has legal rights under applicable national legislation governing the sale of consumer goods and make clear that those rights are not affected by the guarantee and (2) set out in plain intelligible language the contents of the guarantee and the

[1774] Consumer Sales Directive art. 5(2). Sixteen Member States have chosen to provide for such a notification requirement. *See Communication from the Commission to the Council and the European Parliament on the implementation of Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees including analysis of the case for introducing direct producers' liability*, at 9, COM (2007) 210 final (Apr. 24, 2007).

[1775] *See* Consumer Sales Directive art. 1(2)(e) (defining "guarantee" as "any undertaking by a seller or producer to the consumer, given without extra charge, to reimburse the price paid or to replace, repair or handle consumer goods in any way if they do not meet the specifications set out in the guarantee statement or in the relevant advertising").

[1776] *Cf.* Consumer Sales Directive recital 21. For a discussion of these rights see *supra* chapter 5.3.4.

[1777] Consumer Sales Directive art. 6. The prescription of the binding nature of a guarantee was primarily introduced to address particularities in English law. *See* SIMONE JORDEN, VERBRAUCHERGARANTIEN [CONSUMER GUARANTEES] 525 et seq. (2001).

[1778] Consumer Sales Directive art. 6(2).

essential particulars necessary for making claims under the guarantee, notably the duration and territorial scope of the guarantee as well as the name and address of the guarantor.[1779]

Third, on request by the consumer, the guarantee has to be made available in writing or in another durable medium available and accessible to the consumer.[1780]

Furth, a Member State may, if goods are marketed in its own territory, require—in accordance with the rules of the Treaty[1781]—that the guarantee be drafted in one or more official languages of the Community.[1782]

As apparent from the formalistic nature of these requirements, they do little to perform a transfer of information security risks from consumers to software manufacturers.

5.3.6. Comparative Assessment

5.3.6.1. Scope of Application

Negligence tort liability is the type of liability that is not confined to "products" or "goods." On the other hand, strict tort liability under California and New York law as well as the Product Liability Directive only cover "products" while the rules on express and implied warranties under UCC article 2 and the Consumer Sales Directive only cover "goods." All of these liability regimes generally cover software if sold as an integrated part of electronic

[1779] See *id.*

[1780] *See* Consumer Sales Directive art. 6(3). *Cf.* ROBERT BRADGATE & CHRISTIAN TWIGG-FLESNER, CONSUMER SALES AND ASSOCIATED GUARANTEES 178 (2003) (discussing the legal uncertainties associated with the "durable medium" requirement).

[1781] This particularly refers to the prohibition of quantitative restrictions on imports and all measures having equivalent effect under TFEU art. 34 et seq.

[1782] *See* EEC Council Regulation No. 1, art. 1, 1958 O.J. (L 17) 385 (EEC) as amended (stating that "[t]he official languages and the working languages of the institutions of the Union shall be Bulgarian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish").

hardware. When sold without hardware but on a tangible medium, software is often considered a good under UCC article 2 and a "consumer good" under the Consumer Sales Directive. Whether it is a product under the Product Liability Directive and California and New York strict tort liability is less certain. None of the liability regimes focused on "goods" or "products" are likely to cover software that is distributed over the Internet (i.e. not on a tangible medium).

Thus, all of the liability regimes discussed *supra*—with the exception of negligence tort liability under California and New York law—are insufficient in the sense that they only cover software if distributed in certain ways. While understandable from a historical perspective, a distinction that discriminates between different distribution mechanisms is wholly inappropriate when applied to software because the risks associated with the use of a software are independent from the software's distribution mechanism.

Furthermore, UCC article 2 and the Consumer Sales Directive only cover "sales." While UCC article 2 is often also applied to commercial licenses, significant uncertainty exists under the Consumer Sales Directive. However, both liability regimes clearly do not cover software that is given away for free.

This is reasonable as far as non-commercial software is concerned. However, not all free software is non-commercial. Indeed many software products are given away for free because the underlying business model foresees an alternative revenue stream.

For example, Adobe Systems, Inc. makes its Adobe Flash Player freely available because, employing the theory of network effects,[1783] it rightly expects that the value of its content creation software products which are only available for a license fee (e.g. Adobe Flash) will increase along the number of users that are capable of playing content created with that software. Similarly Adobe Reader (used to view PDF files) and Apple QuickTime (used to play movies) are given away for free to create positive network effects for the respective content creation software products Adobe Acrobat and Final Cut Studio which are also only available for a license fee.

The aforementioned free—but commercial—software products are highly significant from a security perspective because (1) they can be found on almost every PC[1784] and (2) severe security vulnerabilities are regularly publicly disclosed for all of them. Between September 1, 2009 and August 31, 2010, 54 highly severe security vulnerabilities were discovered in Adobe Reader, 42 in Adobe Flash Player, and ten in Apple QuickTime.[1785]

While UCC article 2 and the Consumer Sales Directive do not cover free commercial software, strict liability and negligence liability under California and New York law as well as the Product Liability Directive cover such software—to the extent that software is at all considered a "product" for the purposes of strict liability and the Product Liability Directive.

[1783] *Cf.* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 173 et seq. (1999) (explaining that network effects arise when the value one user places on a good depends on how many other people are using it).

[1784] Adobe claims that its Adobe Flash Player is installed on more than 99% of all Internet-enabled PCs. *See* http://www.adobe.com/products/player_census/flashplayer/version_penetration.html (last accessed Feb. 10, 2011). A similar penetration rate is to be expected for Adobe Reader. According to Adobe's (presumably conservative) estimates, Apple's QuickTime has a penetration rate of 57%. *See* http://www.adobe.com/products/player_census/flashplayer/ (last accessed Feb. 10, 2011).

[1785] This data is available via the National Vulnerability Database's advanced search functionality. *See* http://web.nvd.nist.gov/view/vuln/search-advanced?cid=9 (last accessed Sept. 21, 2010).

5.3.6.2. Instances of Liability

UCC article 2 provides liability for a breach of an express or implied warranty of which only the latter can be easily disclaimed. Express warranties include the following if made "part of the basis of the bargain": (1) affirmations of fact or promises made by the seller to the buyer which relate to the goods, (2) any description of the goods, and (3) any sample or model. These three cases could be described as implied contract terms.

The Consumer Sales Directive goes beyond UCC article 2 by providing that conformity with the contract will only be presumed if, in addition to the fulfillment of implied contract terms similar to those of UCC article 2, the goods also meet two objective conditions: (1) fitness for the purposes for which goods of the same type are normally used and (2) showing the quality and performance which are normal in goods of the same type and which the consumer can reasonably expect, taking into consideration, *inter alia*, any public statements made by the producer or the seller.

Strict liability under California and New York law attaches when the manufacturer's product had a defect which was the proximate cause of the plaintiff's injuries. Design defects which are particularly relevant with regard to security vulnerabilities are to be determined using a risk-benefit analysis. Under California law, the expectations of an ordinary consumer may also be considered. Ultimately this is somewhat similar to the Product Liability Directive's standard which focuses on "the safety which a person is entitled to expect."

As discussed *supra*, a "reasonable expectations"-standard whether in the context of contract conformity or product liability brings with it the fundamental challenge that it is inherently unsuitable to change the status quo. If severe security vulnerabilities are discovered on a monthly basis in all major commercial off-the-shelf software products, no consumer will be able to refer to a reasonable expectation of drastically more secure software.

In theory, negligence liability under California and New York law does not suffer from this problem because the defense that everyone else in the industry has equally low security standards is not an absolute defense.[1786] However, in practice courts are not likely to rule that an entire industry—such as the software industry—is acting negligently.

Accordingly, none of the liability regimes, even if fully applied to software irrespective of its method of distribution, is likely to result in a risk transfer that could fundamentally improve the current state of software security.

5.3.6.3. Available Remedies

Strict liability and negligence liability under California and New York law allows the plaintiff to seek damages. However, the economic loss doctrine renders pure economic losses that are most typical with regard to software unrecoverable. Similarly, the Product Liability Directive does not require Member States to provide for the recovery of purely economic losses or immaterial damages. It furthermore prescribes a deductible of €500, thereby eliminating all small claims.

As a remedy, the recovery of damages is ill-suited to address the fact that consumers typically suffer large pure economic losses but rarely property damages or personal injuries due to low levels of software security. If the recovery of pure economic losses were generally permitted,[1787] software manufacturers would face huge financial risks[1788] that, due to the size

[1786] *Cf.* The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) (holding that the fact that most tugboats in the industry do not yet have radios does not prevent the jury for holding that defendant's lack of a radio was negligent).

[1787] *Cf.* Bruce Schneier, *Hacking the Business Climate for Network Security*, IEEE COMPUTER, Apr. 2004, at 87, 88, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 151, 152 (2008) (apparently suggesting that pure economic losses should be recoverable).

[1788] The worm Code Red is estimated to have caused $ 2.6 billion and the worm Blaster $ 2 to 10 billion in damages. *See* George Jones, *The 10 Most Destructive PC Viruses Of All Time*, INFORMATIONWEEK, July 5, of the risks, might be impossible to insure against.[1789] However, if pure economic losses cannot be recovered, as it is currently the case, software manufacturers only bear a very small portion of the risks associated with software vulnerabilities, leaving the fundamental challenge of the misalignment between risk and risk mitigation capability unaddressed.

UCC article 2 allows the available remedies to be limited by contractual means to the return of the goods and the repayment of the price. This remedy is, however, very impractical with regard to most software: First, users are often fully dependent on a particular software (e.g. on Microsoft Office to be able to use all features of Microsoft's document formats).[1790] Second, users may face very high switching costs[1791] that have a prohibitive effect on changing to a different software product.

In this regard, the Consumer Sales Directive has the important advantage over UCC article 2 that it provides not only the rescission of the contract as the only remedy. First, it allows the consumer to require a repair (or a replacement) of the good. Second, it allows the consumer to not only demand the (often impractical) rescission of the contract but, alternatively, to require

2006, http://www.informationweek.com/news/windows/security/showArticle.jhtml?articleID=190300173. For 2006, the global direct financial damage caused by malware was estimated at over $13 billion. *See* COMPUTER ECON., MALWARE REPORT 2007: THE ECONOMIC IMPACT OF VIRUSES, SPYWARE, ADWARE, BOTNETS AND OTHER MALICIOUS CODE 5 (2007), *available at* http://www.computereconomics.com/article.cfm?id=1224.

[1789] Rainer Böhme & Gaurav Kataria, *On the Limits of Cyber-Insurance*, *in* TRUST AND PRIVACY IN DIGITAL BUSINESS 31 (Simone Fischer-Hübner et al. eds., 2006) (showing that there may not be a market solution for globally correlated risks from the worldwide spread of a worm or virus, as the insurer's cost of safety capital becomes too high).

[1790] OpenOffice does not fully implement Microsoft Office's document format Office Open XML. *See* http://wiki.services.openoffice.org/wiki/Documentation/FAQ/General/How_do_I_open_Microsoft_Office_2007_files%3F (last accessed Feb. 10, 2011).

[1791] Two examples of switching costs are: (1) having thousands of files that cannot be properly interpreted by the new software; and (2) having to learn to use the new software's menu system which may significantly differ from the old. *Cf.* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 117, 285 (1999).

a reduction of the price. It is this last remedy that seems particularly well suited to adequately ensure accountability of software manufacturers with regard to pure economic losses.

5.3.6.4. Conclusion

Making software manufacturers liable for the insufficiently low levels of security of their products constitutes a direct risk transfer from the users to the software manufacturers.[1792] Such a risk transfer is appropriate to address the fundamental problem that the risks associated with low software security are currently mostly borne by the users who are not capable of significantly mitigating these risks.[1793] To align risk and risk mitigation capability, some form of liability is needed.[1794]

However, none of the liability regimes discussed *supra* effectively addresses the issue of software security. By limiting their scope to tangible products or goods, defining instances of liability that only cover very few security vulnerabilities, or limiting the available remedies, they all fail to sufficiently transfer the risks associated with inadequate software security to the software manufacturers.

5.4. Limiting the Liability of Payment Service Users

All companies that offer payment services, whether in the form of a credit card, ATM card, or an online payment service, require their users to authenticate themselves in order to use the

[1792] *See supra* chapter 3.2.3.1.

[1793] *See supra* chapter 2.4.4.

[1794] *Cf.* Bruce Schneier, *Make Vendors Liable for Bugs*, WIRED, June 6, 2006, http://www.wired.com/politics/security/commentary/securitymatters/2006/06/71032, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 147 (2008); NAT'L RESEARCH COUNCIL, CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 14 (2002) (stating that policy makers should "[c]onsider legislative responses to the failure of existing incentives to cause the market to respond adequately to the security challenge. Possible options include steps that would increase the exposure of software and system vendors […] to liability for system breaches").

payment service. Typically that authentication is at least partly based on something the user knows. If the confidentiality of that information is compromised, a malicious third party may use it to initiate fraudulent transactions. The security and, more specifically, confidentiality of information that is used to authenticate a user is therefore of great importance.

There are typically many vulnerabilities that allow the confidentiality of such authenticating information to be compromised. First, the authenticating information may be plainly written on a plastic card (in particular a credit card). Second, it may be stored electronically on a card but not sufficiently protected by cryptographic means.[1795] Third, once the authenticating information is given to a merchant, the systems he uses to store, process, and transmit the information may contain a whole range of vulnerabilities.

These vulnerabilities can only be properly addressed by payment service providers and merchants.[1796] To avoid a misalignment between risk and risk mitigation capability, these entities should therefore bear most of the risks associated with the confidentiality of information that authenticates users of payment services.

However, it would typically be easy to for payment service providers to use contractual means to ultimately transfer the risk of fraudulent transactions to the users—that is if a regulatory policy does not limit the liability of users, thereby reversing the risk transfer.

[1795] *Cf.* ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 80, 199 (2d ed. 2008).

[1796] While the payment service providers could issue more secure cards or perform automatic fraud detection, merchants could generally improve their information security stance.

5.4.1. The Limitation of Liability of Payment Service Users in the U.S.

In the U.S., the Truth in Lending Act[1797] and the Electronic Fund Transfer Act[1798] drastically limit the liability of holders of a credit card, an ATM card, or a debit cards.

Section 133(a) of the Truth in Lending Act[1799] protects credit card holders against losses due to theft or fraudulent use of credit cards "on the theory that the card issuer is in the better position to prevent such losses."[1800] Specifically, a cardholder's liability for unauthorized uses of his credit card is limited to $50.[1801] Furthermore, a cardholder faces no liability at all if only the credit card number but not the credit card itself was misused for the fraud.[1802]

As regards unauthorized "electronic fund transfers,"[1803] in particular those that are authorized by a debit card or an ATM card, Electronic Fund Transfer Act § 909(a)[1804] generally limits an individual's[1805] liability to $50.[1806] This limit does not apply if the individual fails to report

[1797] Truth in Lending Act, Pub. L. No. 90-321, Title I, 82 Stat. 146 (1968) (codified as amended at 15 U.S.C. § 1601-1667f).

[1798] Electronic Fund Transfer Act, Pub. L. No. 95-630, Title XX, 92 Stat. 3641, 3728 (1978) (codified as amended at 15 U.S.C. §§ 1693-1693r).

[1799] 15 U.S.C. § 1643(a) (2010).

[1800] Minskoff v. Am. Exp. Travel Related Services Co., Inc., 98 F.3d 703, 708-09 (2d Cir. 1996).

[1801] *See* 15 U.S.C. § 1643(a)(1)(B) (stating that one of the conditions for any cardholder liability is that "the liability is not in excess of $50"). *Cf. also* 12 C.F.R. § 226.12(b)(2).

[1802] The Federal Reserve Board's Official Staff Interpretations, codified at 12 C.F.R. pt. 226, Supp. I explicitly state that "when merchandise is ordered by telephone or the Internet by a person without authority to do so, using a credit card account number by itself or with other information that appears on the card (for example, the card expiration date and a 3- or 4-digit cardholder identification number), no liability may be imposed on the cardholder."

[1803] *See* 15 U.S.C. § 1693a(6) (defining "electronic fund transfers" as "any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account").

[1804] 15 U.S.C. § 1693g(a) (2010).

[1805] 15 U.S.C. § 1693g(a) uses the term "consumer" which is defined in 15 U.S.C. § 1693a(5) as "a natural person."

within 60 days of transmittal of his account statement any fraudulent transactions that appear on that statement or does not report any loss or theft of a card or other means of authentication within two business days.[1807] However, in no event is an individual liable for fraudulent transactions initiated after the financial institution has been notified of the loss or theft of a means of authentication.[1808]

5.4.2. The Limitation of Liability of Payment Service Users in the EU

Parliament and Council Directive 2007/64[1809] (hereinafter *Payment Services Directive* or *PSD*) generally limits a consumer's[1810] liability for unauthorized payment transactions to €150.[1811] This liability cap does not apply if the consumer acted fraudulently[1812] or, acting with intent or gross negligence,[1813] failed to notify the payment service provider without undue delay on becoming aware of loss, theft, misappropriation, or unauthorized use of the payment instrument.[1814] Furthermore, the liability cap is also not applicable if the consumer

[1806] 15 U.S.C. § 1693g(a)(1).

[1807] *See* 15 U.S.C. § 1693g(a). If an individual fails to report the theft or loss of his card (or other means of authentication) within two business days but does notify the financial institution of fraudulent transactions within 60 days of transmittal of his account statement, liability is limited to $500. *See* 12 C.F.R. § 205.6(b)(2).

[1808] *See* 15 U.S.C. § 1693g(a).

[1809] 2007 O.J. (L 319) 1 (EC) as amended by Parliament and Council Directive 2009/111, art. 3, 2009 O.J. (L 302) 97, 118 (EC). For a general comparison of the legal regimes for payment services in the EU and the U.S. see Benjamin Geva, *Payment Transactions Under the EU Payment Services Directive: A U.S. Comparative Perspective*, 27 PENN ST. INT'L L. REV. 713 (2009).

[1810] PSD art. 61 indeed applies to all "payers" (as broadly defined in PSD art. 4(7). However, pursuant to PSD art. 51(1), art. 61 can be contracted out of if the payer is not a "consumer." *Cf.* PSD art. 4(11) (defining "consumer" as "a natural person who, in payment service contracts covered by this Directive, is acting for purposes other than his trade, business or profession").

[1811] PSD art. 61(1).

[1812] *See* PSD art. 61(2).

[1813] *Cf.* PSD art. 61(3) (providing that Member States "may" reduce the payer's liability in cases of gross negligence).

[1814] *See* PSD art. 61(2) in conjunction with PSD art. 56(1)(b).

violated the terms governing the use of the payment instrument,[1815] in particular by failing to "take all reasonable steps to keep its personalized security features safe."[1816]

Lastly, unless a consumer acted fraudulently, he does not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after he has provided proper notice to the payment service provider.[1817]

5.4.3. Comparative Assessment

The Truth in Lending Act categorically limits liability to $50 in cases of unauthorized use of a credit card and entirely eliminates any liability if only the credit card information (and not the credit card) was misused.[1818]

The Electronic Fund Transfer Act and the Payment Service Directive, on the other hand, only provide limited liability if the individual notifies the financial institution within certain time frames. Given that large fraudulent transactions are very likely to be noticed and acted upon by an account holder, this requirement for limited liability may be less significant in practice.

What seems more significant is that the Payment Service Directive sets the liability cap at €150, more than three times that of the Truth in Lending Act and Electronic Fund Transfer

[1815] *See* PSD art. 61(2) in conjunction with PSD art. 56(1)(a).

[1816] PSD art. 56(2).

[1817] PSD art. 61(4) (referring to art. 56(1)(b)). This does not apply "if the payment instrument does not allow its blocking or prevention of its further use." PSD art. 53(a).

[1818] Note that many consumers seem to be unaware of this limited liability. In a recent survey, 57% stated that they were either "extremely concerned" or "very concerned" about the "theft" of credit card information. *See* IDENTITY THEFT RES. CTR., 1ST ANNUAL IDENTITY THEFT RESOURCE CENTER "CONSUMER INTERNET TRANSACTION CONCERNS" SURVEY 2 (2010), http://www.idtheftcenter.org/artman2/uploads/1/Consumer_Concerns_Survey_20100813.pdf.

Act. The liability limitations under U.S. law are therefore ultimately stronger than those under EU law.

U.S. law as well as EU law, albeit to a different extent, limit the liability of users of payment services and thereby perform an important risk transfer from the users of a payment service to the providers of such services. In doing so, U.S. and EU law reverses a risk transfer that would otherwise be performed by contractual means to the detriment of consumers.

This transfer of risk by way of limited liability effectively addresses the fundamental challenge of the misalignment between risk and risk mitigation capability[1819] as applied to the security of payment services. It ensures that those entities capable of mitigating the risks presented (the payment service providers) also bear most of the risks.[1820]

It is this regulatory environment that led to the creation of arguably the most successful self-regulatory instrument in the area of information security: the Payment Card Industry Data Security Standard (PCI DSS).[1821] The PCI DSS is a worldwide information security standard developed by the Payment Card Industry Security Standards Council[1822] and is contractually

[1819] *See supra* chapter 2.4.4.

[1820] *Cf.* MICHEL J.G. VAN EETEN & JOHANNES M. BAUER, OECD, ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES, DSTI/DOC(2008)1, at 35 (2008), *available at* http://www.oecd.org/dataoecd/53/17/40722462.pdf (noting the importance of fraud losses as an incentive for payment service providers to improve security).

[1821] PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES, VERSION 2.0 (2010), *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf. *Cf.* Mark MacCarthy, *Payment Card Industry Data Security Standard, in* PROSKAUER ON PRIVACY § 16:2.2 (Kristen J. Mathews ed., 2010) (noting that the development of PCI DSS can be traced to the regulatory allocations of fraud losses which has provided "a powerful incentive for card companies to minimize unauthorized use of cards").

[1822] The PCI Security Standards Council was founded in 2006. *See* https://www.pcisecuritystandards.org/organization_info/index.php (last accessed Feb. 10, 2011).

imposed by the credit card brands which founded the Council[1823] on all merchants or other entities that process cardholder information.[1824] While PCI DSS has been widely implemented and enforced in the U.S., its implementation in the EU has only started as recently as September 2010.[1825]

PCI DSS requires the implementation of numerous specific security controls by establishing twelve general requirements[1826] and over 210 sub-requirements.[1827] Since PCI DSS is not a regulatory instrument, a risk-based assessment of PCI DSS is beyond the scope of this thesis.[1828] From a regulatory perspective, it is sufficient to emphasize that the credit card

[1823] These are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. *See id*. Note that Visa Europe is a separate, independently operating company which is owned by its European member financial institutions. *See* http://corporate.visa.com/about-visa/our-business/visa-inc-and-visa-europe.shtml (last accessed Feb. 10, 2011).

[1824] Note that Visa and Mastercard do not have direct contractual relationships with cardholders and merchants; they only have contractual relationships with (1) card issuing banks ("issuers") who provide payment cards to cardholders and (2) acquiring banks which sign up merchants to accept payment cards. *See* Mark MacCarthy, *Payment Card Industry Data Security Standard, in* PROSKAUER ON PRIVACY § 16:2.1 (Kristen J. Mathews ed., 2010). Visa and Mastercard therefore have to contractually obligate acquiring banks to, in turn, contractually impose PCI DSS on merchants.

[1825] *See* Ron Condon, *Exclusive PCI DSS news: EU regional director rallies UK merchants*, SEARCHSECURITY.CO.UK, Jul. 9, 2010, http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1516495,00.html (noting that UK merchants that process more than six million transactions annually and accept Visa or MasterCard must comply with PCI DSS by the end of September 2010).

[1826] These twelve requirements are: (1) install and maintain a firewall configuration to protect cardholder data; (2) do not use vendor-supplied defaults for system passwords and other security parameters; (3) protect stored cardholder data; (4) encrypt transmission of cardholder data across open, public networks; (5) use and regularly update anti-virus software or programs; (6) develop and maintain secure systems and applications; (7) restrict access to cardholder data by business need to know; (8) assign a unique ID to each person with computer access; (9) restrict physical access to cardholder data; (10) track and monitor all access to network resources and cardholder data; (11) regularly test security systems and processes; and (12) maintain a policy that addresses information security for all personnel. *See* PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES, VERSION 2.0 (2010), *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

[1827] *See id*.

[1828] Note, however, that most of the criticism of PCI DSS comes from merchants who naturally feel burdened by having to protect cardholder information. In particular, such critics have argued that PCI DSS contains a great number of sub-requirements "some of which can place an incredible burden on a retailer and many of which are subject to interpretation." *Do the Payment Card Industry Data Standards Reduce Cybercrime?: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity and Science and Technology of the H. Comm. on Homeland Security*, 111th Cong. 37 (2009) (statement of Richard Jones, Senior Vice President and Chief Information brands organized in the PCI Security Standards Council do not only have the capability to mitigate information security risks to cardholder information by improving PCI DSS, they also bear the risk that PCI DSS may indeed not be sufficiently effective.

Officer of Michaels Stores, Inc.). *Cf. also* Marc L. Songini, *Retailers fume over PCI security rules*, COMPUTERWORLD, June 7, 2007, http://www.computerworld.com/s/article/9023998/Retailers_fume_over_PCI_security_rules. Remarkably, PCI DSS is regularly criticized by referring to data security breaches as proof for the fact that it does not provide 100% security (as if 100% security was indeed achievable; *see supra* chapter 1). *Cf.* Greg Reber, *PCI compliance falls short of assuring website security*, SEARCHSOFTWAREQUALITY.COM, Oct. 27, 2008, http://searchsoftwarequality.techtarget.com/news/column/0,294698,sid92_gci1335662,00.html; *PCI Update: Compliant Does Not Mean Secure*, SECUREWORKS' ON THE RADAR NEWSLETTER (SecureWorks, Inc., Ga.), Mar. 2009, http://www.secureworks.com/research/newsletter/2009/03/#pci. These (and other) criticisms are particularly well addressed by ANTON A. CHUVAKIN & BRANDEN R. WILLIAMS, PCI COMPLIANCE: UNDERSTAND AND IMPLEMENT EFFECTIVE PCI DATA SECURITY STANDARD COMPLIANCE 324, 326, 328, 336 (2d ed. 2010) (arguing that the following commonly held beliefs are indeed unfounded: PCI DSS is too onerous, breaches prove PCI DSS irrelevant, PCI DSS is all that is needed for security, PCI DSS is toothless). The only formal study conducted on the issue of PCI DSS's effectiveness shows a mixed picture. *See* PONEMON INST., 2009 PCI DSS COMPLIANCE SURVEY 12 (2009), *available at* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/PCI%20DSS%20Survey%20Key%20Findings%20FINAL4.pdf (finding that 44% of respondents "strongly agree" or "agree" that compliance with PCI DSS improves the organization's data security).

6. Regulating Information Security by Mandating Transparency

Regulatory policies that aim at creating transparency with regard to information security are potentially of great value since they may not only address the fundamental challenge of uninformed risk decisions[1829] but may also, in a less obvious fashion, address the challenge of the misalignment between risk and risk mitigation capability: as explained in chapter 3.2.3.2, targeted transparency policies potentially allow customers (or other actors to which the security-related information is disclosed) to take information security aspects into account when making their buying decisions, thereby transferring part of the risks associated with low levels of security to those actors that are subject to the disclosure obligations.

The first three of the following chapters discuss regulatory policies that mandate certain disclosures: vulnerability disclosure by publicly traded companies (see *infra* chapter 6.1), data security breach notification (see *infra* chapter 6.2), and network security breach notification (see *infra* chapter 6.3). Lastly, chapter 6.4 addresses the importance of the accuracy of voluntarily disclosed information by discussing regulatory policies that prohibit deceptive advertising.

6.1. Mandatory Vulnerability Disclosure for Publicly Traded Companies

When making decisions about whether to buy or sell shares in publicly traded companies, investors rely on the integrity of the information reported by those companies. To address the risks to the integrity of reported information, a regulatory regime may aim at (indirectly) mitigating these risks by requiring the implementation of safeguards.[1830] An alternative

[1829] *See supra* chapter 2.4.3.

[1830] *See supra* chapter 4.2.

approach, which is of interest here, consists of mandating the disclosure of vulnerabilities that could result in the loss of integrity.

6.1.1. Sarbanes-Oxley Act of 2002

As discussed in chapter 4.2.1, the Sarbanes-Oxley Act of 2002 (SOX)[1831] requires publicly traded companies to implement "internal controls." Additionally, and more important for the discussion in this chapter, it also mandates that publicly traded companies report on their assessment of these "internal controls."

SOX § 302(4)[1832] requires with regards to "disclosure controls and procedures"[1833] that the CEO and CFO certify in each annual or quarterly report filed or submitted under § 13(a) or § 15(d) of the Securities Exchange Act of 1934[1834] that they (1) have evaluated the effectiveness of the disclosure controls as of a date within 90 days prior to the report; and (2) have presented in the report their conclusions about the effectiveness of the disclosure controls based on their evaluation as of that date.[1835]

[1831] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified in scattered Sections of 11, 15, 18, 28 and 29 U.S.C.)

[1832] 15 U.S.C. § 7241(4).

[1833] 17 C.F.R. §§ 240.13a-15(e) and 240.15d-15(e) (defining "disclosure controls and procedures" as "controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the [Securities Exchange Act of 1934] is recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms"). *Cf.* chapter 4.2.1 (discussing the distinction between "disclosure controls and procedures" and "internal control over financial reporting").

[1834] Securities Exchange Act of 1934, 48 Stat. 881 (codified at 15 U.S.C. § 78a et seq.).

[1835] *Cf.* 17 C.F.R. §§ 240.13a-15(b), 240.15d-15(b) (stating that each such issuer's management must evaluate, with the participation of the issuer's CEO and CFO, the effectiveness of the issuer's disclosure controls and procedures, as of the end of each fiscal quarter). *Cf. also* Regulation S-K, Item 307, 17 C.F.R. § 229.307 (stating that an issuer must disclose the conclusions of the CEO and CFO, regarding the effectiveness of the disclosure controls and procedures).

It has to be emphasized that with regard to disclosure controls, a self-evaluation (as opposed to an independent third-party evaluation) is sufficient. A particular evaluation procedure does not have to be followed either. Under the rules promulgated by the SEC, an issuer only has to "develop a process that is consistent with its business and internal management and supervisory practices."[1836]

The requirements regarding "internal control over financial reporting,"[1837] on the other hand, are decidedly more stringent and have consequently been the focal point of all SOX compliance efforts.

SOX § 404(a) directs the SEC to promulgate rules requiring each annual report to contain an "internal control report" that, *inter alia*, contains "an assessment […] of the effectiveness of the internal control structure and procedures of the issuer for financial reporting."[1838]

The most critical provision, however, is SOX § 404(b). Due to significant criticism regarding its burden on smaller public companies,[1839] the Dodd-Frank Wall Street Reform and Consumer Protection Act[1840] narrowed its personal scope of application to "large accelerated

[1836] Certification of Disclosure in Companies' Quarterly and Annual Reports; Final Rule, 67 Fed. Reg. 57,276, 57,280 (Sept. 9, 2002).

[1837] *See* 17 C.F.R. §§ 240.13a-15(f) and § 240.15d-15(f) (defining "internal control over financial reporting" as "a process […] to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles […]"). *Cf.* chapter 4.2.1 (discussing the distinction between "disclosure controls and procedures" and "internal control over financial reporting").

[1838] SOX § 404(a), 15 U.S.C. § 7262(a).

[1839] For an overview of the discussion see John L. Orcutt, *The Case Against Exempting Smaller Reporting Companies from Sarbanes-Oxley Section 404: Why Market-Based Solutions Are Likely to Harm Ordinary Investors*, 14 FORDHAM J. CORP. & FIN. L. 325 (2009); Paul P. Arnold, *Give Smaller Companies A Choice: Solving Sarbanes-Oxley Section 404 Inefficiency*, 42 U. MICH. J.L. REFORM 931 (2009).

[1840] Pub. L. No. 111-203, § 989G(a) 124 Stat. 1376, 1948 (2010) (to be codified at SOX § 404(c), 15 U.S.C. 7262(c)).

filers"[1841] and "accelerated filers."[1842] SOX § 404(b) requires that a registered public accounting firm makes an attestation of the assessment made by the issuer's management. In doing so, the public accounting firm has to follow standards for attestation engagements issued by the Public Company Accounting Oversight Board (PCAOB).[1843]

Under Item 308 of Regulation S-K issued by the SEC,[1844] the internal control report must contain, *inter alia*, (1) a statement identifying the evaluation framework used by management and (2) management's assessment of the effectiveness of the internal control over financial reporting, including a statement as to whether or not the control is effective.[1845] The assessment must include the disclosure of any "material weakness"[1846] which precludes

[1841] *See* 17 C.F.R. § 240.12b-2(2) (defining "large accelerated filer" as "an issuer after it first meets the following conditions as of the end of its fiscal year: (i) The issuer had an aggregate worldwide market value of the voting and non-voting common equity held by its non-affiliates of $700 million or more, as of the last business day of the issuer's most recently completed second fiscal quarter; (ii) The issuer has been subject to the requirements of section 13(a) or 15(d) of the Act for a period of at least twelve calendar months; (iii) The issuer has filed at least one annual report pursuant to section 13(a) or 15(d) of the Act; and (iv) The issuer is not eligible to use the requirements for smaller reporting companies in Part 229 of this chapter for its annual and quarterly reports.").

[1842] *See* 17 C.F.R. § 240.12b-2(1) (defining "accelerated filer" as "an issuer after it first meets the following conditions as of the end of its fiscal year: (i) The issuer had an aggregate worldwide market value of the voting and non-voting common equity held by its non-affiliates of $ 75 million or more, but less than $ 700 million, as of the last business day of the issuer's most recently completed second fiscal quarter; (ii) The issuer has been subject to the requirements of section 13(a) or 15(d) of the Act (15 U.S.C. 78m or 78o(d)) for a period of at least twelve calendar months; (iii) The issuer has filed at least one annual report pursuant to section 13(a) or 15(d) of the Act; and (iv) The issuer is not eligible to use the requirements for smaller reporting companies in Part 229 of this chapter for its annual and quarterly reports.").

[1843] The PCAOB has been established by SOX § 101, 15 U.S.C. § 7211. The PCAOB is not an agency or establishment of the United States Government but a nonprofit corporation. *Id.* § 7211(b). However, it has been vested with the power to adopt rules and register, inspect and discipline registered public accountants. This led to constitutional challenges of the establishment of PCAOB. *Cf.* HAROLD S. BLOOMENTHAL, SARBANES-OXLEY ACT IN PERSPECTIVE § 2:1 et seq. (2009). *See* Free Enter. Fund v. Pub. Co. Accounting Oversight Bd., 130 S. Ct. 3138, 3161 (2010) (holding that the existence of the PCAOB does not violate the separation of powers, but the substantive removal restrictions (only "for good cause") do).

[1844] 17 C.F.R. § 229.308 (2010). Item 308 was introduced in 2003. *See* Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports; Final Rule, 68 Fed. Reg. 36,636 (June 18, 2003).

[1845] 17 C.F.R. § 229.308(a)(2) and (3).

[1846] *See infra.*

management from concluding that the internal control over financial reporting is effective.[1847] "Significant deficiencies"[1848] that do not amount to material weaknesses only have to be disclosed to the issuer's auditors and the audit committee of the board of directors but not to the public.[1849] Finally, the internal control report must also contain the registered public accounting firm's attestation report.[1850]

As stated above, SOX § 404(b) provides that public accounting firms have to follow standards issued by the PCAOB when issuing an attestation report. In 2004, the PCAOB issued Auditing Standard No. 2 (AS No. 2)[1851] which was superseded by Auditing Standard No. 5 (AS No. 5)[1852] in 2007. Following the interpretive guidance issued by the SEC,[1853] AS No. 5 implemented a risk-based top-down[1854] audit approach as its organizing principle.[1855] This

[1847] *Id.* § 229.308(a)(3).

[1848] *See* 17 C.F.R. §§ 210.1–02(4), 240.12b–2 (defining "significant deficiency" as "a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the registrant's financial reporting").

[1849] *See* SOX § 303(a)(5)(A), 15 U.S.C. § 7241(a)(5)(A). *Cf.* JOHN T. BOSTELMAN, 1 THE SARBANES-OXLEY DESKBOOK §§ 4:4.5 et seq., 5:1.3[B][3] (2009).

[1850] *Id.* § 229.308(b).

[1851] PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING PERFORMED IN CONJUNCTION WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 2, RELEASE NO. 2004-001 (2004). AS No. 2 was approved by the SEC pursuant to SOX § 107(b), 15 U.S.C. § 7217(b), on June 17, 2004. *See* Securities Exchange Act Release No. 49884, 69 Fed. Reg. 35083 (June 17, 2004).

[1852] PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A (2007). AS No. 5 was approved by the SEC on July 27, 2007. *See* Securities Exchange Act Release No. 34-56152, 72 Fed. Reg. 42,141 (July 27, 2007).

[1853] Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934; Final Rule, 72 Fed. Reg. 35,324 (June 27, 2007).

[1854] Compliance efforts under AS No. 2 have often followed a bottom-up approach not based on risk. Assessments therefore often became a labor-intensive, mechanistic check-the-box exercise. *See* SEC, DIV. OF CORPORATION FINANCE & OFFICE OF THE CHIEF ACCOUNTANT, STAFF STATEMENT ON MANAGEMENT'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING 5 (2005), *available at* http://sec.gov/info/accountants/stafficreporting.pdf. *Cf.* Donald C. Langevoort, *Symposium: Robert Clark's Corporate Law: Twenty Years of* requires auditors to first focus on entity-level controls before assessing lower level controls. Entity-level controls include the issuer's risk assessment process, centralized processing and controls, controls to monitor results of operations, and controls to monitor other controls.[1856] AS No. 5 is also strongly focused on the concept of "material weaknesses" as it does not require an auditor to search for deficiencies that, individually or in combination, are less severe than a material weakness.[1857]

The rules promulgated by the SEC require the management of an issuer to use a control framework that is "suitable, recognized [and] is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment."[1858] AS No. 5 mandates that the auditor uses the same control framework as the management.[1859] In practice, the COSO control framework,[1860] which the SEC has declared to

Change: Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's "Duty of Care as Responsibility for Systems", 31 IOWA J. CORP. L. 949, 966 (2006) (describing the inflated construction of § 404's requirements as rent-seeking by auditors and attorneys). *Cf. also* Clinton W. Rancher, Note, *More Art Than Science: The State-of-the-Art in Fraud Risk Assessment and Its Implications for Auditing Standard No. 5*, 6 GEO. J.L. & PUB. POL'Y 371, 376 (2008) (emphasizing the importance of a strategic risk assessment).

[1855] PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A, at 6, A1-11 (2007).

[1856] PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A, at A1-13 (2007). *Cf.* MICHAEL J. RAMOS, HOW TO COMPLY WITH SARBANES-OXLEY SECTION 404: ASSESSING THE EFFECTIVENESS OF INTERNAL CONTROL 54 et seq. (2008)

[1857] PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A, at A1-26 (2007). However, significant deficiencies that do not amount to material weaknesses nevertheless have to be reported to the audit committee. Non-significant deficiencies have to be reported to management. *Id.* at 11, 31.

[1858] 17 C.F.R. §§ 240.13a-15(c), 240.15d-15(c).

[1859] PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A, at A1-5 (2007).

[1860] COMM. OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMM'N [COSO], INTERNAL CONTROL—INTEGRATED FRAMEWORK (1992). *Cf.* JAMES HAMILTON & PETER RASMUSSEN, GUIDE TO INTERNAL CONTROLS UNDER SECTION 404 OF THE SARBANES-OXLEY ACT 51 (2d ed. 2007).

fulfill the regulatory requirements,[1861] is widely accepted as the industry standard among large public companies.[1862] Other well known control frameworks, albeit limited to information technology, are the ITIL[1863] (dealing with IT service management) and COBIT.[1864]

From a practical perspective, the most important issue is whether the auditor identifies a "material weakness" in the internal control over financial reporting.[1865] This is because material weaknesses have to be disclosed by management in the annual internal control report,[1866] where the disclosure should include information about: (1) the nature of the material weaknesses; (2) their impact on the issuer's financial reporting; and (3) management's current plans, if any, or actions already undertaken, for remediating the material weakness.[1867] In addition, as mentioned above, a material weakness bars management from finding that internal control over financial reporting is "effective."[1868]

[1861] Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports; Final Rule, 68 Fed. Reg. 36,636, 36,642 (stating that "[t]he COSO Framework satisfies our criteria and may be used as an evaluation framework").

[1862] *Cf.* SANJAY ANAND, SARBANES-OXLEY GUIDE FOR FINANCE AND INFORMATION TECHNOLOGY PROFESSIONALS 47 (2006).

[1863] U.K. OFFICE OF GOVERNMENT COMMERCE, INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY V3 (2007). *Cf.* ROBERT R. MOELLER, SARBANES-OXLEY INTERNAL CONTROLS: EFFECTIVE AUDITING WITH AS5, COBIT, AND ITIL 203 et seq. (2008).

[1864] IT GOVERNANCE INST., CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT) 4.1 (2007), *available at* http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf. *Cf.* ROBERT R. MOELLER, SARBANES-OXLEY INTERNAL CONTROLS: EFFECTIVE AUDITING WITH AS5, COBIT, AND ITIL 119 et seq. (2008).

[1865] An auditor is not required to search for deficiencies that, individually or in combination, are less severe than a material weakness. *See* PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A, at A1-26 (2007).

[1866] 17 C.F.R. § 229.308(a)(3).

[1867] Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, 72 Fed. Reg. 35324, 35333 (June 27, 2007).

[1868] 17 C.F.R. § 229.308(a)(3).

The term "material weakness" is defined in the SEC rules as "a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of the registrant's annual or interim financial statements will not be prevented or detected on a timely basis."[1869] AS No. 5 also adopted this definition[1870] and further provides that an auditor must evaluate the severity of each control deficiency[1871] that comes to her attention, taking into account (1) whether there is more than a remote likelihood[1872] that the issuer's controls will fail to prevent or detect a misstatement of an account balance or disclosure; and (2) the magnitude of the potential misstatement resulting from the deficiency or deficiencies.[1873]

In summary, the purpose of SOX § 404(b) is therefore the third party assessment of internal control over financial reporting to identify material weaknesses that have more than a remote likelihood of leading to material misstatement in the financial statements.[1874] This in turn ensures that material weaknesses are disclosed to the public in the annual internal control

[1869] 17 C.F.R. §§ 210.1–02(4), 240.12b–2.

[1870] PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A, at A1-43 (2007).

[1871] *See id.*, at A1-41 (stating that a deficiency exists "when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis").

[1872] *Id.* at A1-43 uses the term "reasonable possibility" which it defines as an event being either "reasonably possible" or "probable," as defined in FIN. ACCOUNTING STANDARDS BD., *ACCOUNTING FOR CONTINGENCIES*, STATEMENT OF FINANCIAL ACCOUNTING STANDARDS NO. 5, at 4 (1975) (defining three terms to describe probability: probable ["future event or events are likely to occur"], reasonably possible ["chance of the future event or events occurring is more than remote but less than likely"], and remote ["chance of the future event or events occurring is slight"]). For a critical discussion of such qualitative risk assessment methods see *supra* chapter 4.1.10.4.

[1873] PCAOB, AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A, at A1-26 (2007).

[1874] *Cf.* Peter Ferola, *Internal Controls in the Aftermath of Sarbanes-Oxley: One Size Doesn't Fit All*, 48 S. TEX. L. REV. 87, 94 (2006). *Cf. also* Donald C. Langevoort, *Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's "Duty of Care As Responsibility for Systems"*, 31 J. CORP. L. 949, 956 (2006).

reports. However, the assessment effectively requires a qualitative—rather than quantitative—risk assessment which brings with it all the problems discussed *supra* in chapter 4.1.10.4.

As discussed *supra* in chapter 4.2.1, SOX provides very strong enforcement mechanisms by holding senior managers personally accountable. A failure to disclose a material weakness in the annual internal control report can result in liability to any person who, in reliance upon the statement, has purchased or sold a security at a price which was affected by the statement.[1875] Furthermore knowing violations can lead to criminal penalties of up to $1,000,000 or imprisonment of up to 10 years, or both.[1876] For willful violations, the penalty is increased to up to $5,000,000, or imprisonment of up to 20 years, or both.[1877] The SEC may also seek redress,[1878] which includes the possibility of cease-and-desist proceedings to prohibit individuals from serving as directors or officers of public companies.[1879]

Compliance with SOX §§ 302, 404, and with § 404(b) in particular, has been rather costly for many issuers,[1880] at least to some extent due to misguided practices of audit firms.[1881] This has prompted the SEC, with respect to § 404(b), to defer the compliance date for non-accelerated

[1875] Securities Exchange Act of 1934 §§ 13(a) and 18, 15 U.S.C. § 78m(a) and 78r.

[1876] SOX § 906, 18 U.S.C. § 1350.

[1877] 18 U.S.C. § 1350(c)(2).

[1878] *See* Securities Exchange Act of 1934 §§ 20, 21, 21C and 21D, 15 U.S.C. §§ 78t, 78u, 78u–3 and 78u–4.

[1879] *See* 15 U.S.C. § 78u-3. *Cf.* JOHN T. BOSTELMAN, 2 THE SARBANES-OXLEY DESKBOOK § 15:1 et seq. (2009).

[1880] *Cf.* SEC, OFFICE OF ECONOMIC ANALYSIS, STUDY OF THE SARBANES-OXLEY ACT OF 2002 SECTION 404 INTERNAL CONTROL OVER FINANCIAL REPORTING REQUIREMENTS (2009), *available at* http://www.sec.gov/news/studies/2009/sox-404_study.pdf. *Cf. also* John C. Coffee, *Law and the Market: The Impact of Enforcement*, 156 U. PA. L. REV. 229, 241-42 (2007); Robert Prentice, *Sarbanes-Oxley: The Evidence Regarding the Impact of Sox 404*, 29 CARDOZO L. REV. 703, 729-30 (2007); Roberta Romano, *Does the Sarbanes-Oxley Act Have A Future?*, 26 YALE J. ON REG. 229, 251 (2009).

[1881] Charles W. Murdock, *Sarbanes-Oxley Five Years Later: Hero or Villain*, 39 LOY. U. CHI. L.J. 525, 552 (2008) (noting that "[s]ome of the outlandish costs associated with Section 404 compliance are not a problem of government regulation, but rather a problem within […] the accounting profession").

filers[1882] to 2010[1883] and, ultimately, Congress to limit § 404(b)'s personal scope of application to accelerated filers and large accelerated filers.[1884]

Overall, the mandatory disclosure of information regarding (1) the effectiveness of "disclosure controls and procedures" under SOX § 302 and (2) the effectiveness and material weaknesses of "internal control over financial reporting" under SOX § 404 allows investors to make more informed investment decisions, taking into account the level of integrity of disclosed information, as indicated in particular by any material weaknesses disclosed. Lastly, it is important to note that empirical evidence suggests that the requirement of an independent audit—which is only required under SOX § 404 and only for accelerated filers and large accelerated filers—is central to an effective disclosure regime.[1885]

6.1.2. EU Statutory Audit Directive

Parliament and Council Directive 2006/43[1886] (hereinafter *Statutory Audit Directive*)[1887] was adopted to harmonize statutory audit requirements in the EU.[1888] Due to the fact that it

[1882] *Cf. supra* note 1842 (providing a definition for the term "accelerated filer").

[1883] Non-accelerated filers will have to begin complying in their first annual report for fiscal years ending on or after June 15, 2010. *See* Commissioner Luis A. Aguilar, Statement of Commissioner Luis A. Aguilar Regarding His Commitment to Implementation of Sarbanes-Oxley Section 404(b) (Oct. 2, 2009) (transcript available at http://www.sec.gov/news/speech/2009/spch100209laa.htm). *Cf.* John L. Orcutt, *The Case Against Exempting Smaller Reporting Companies from Sarbanes-Oxley Section 404: Why Market-Based Solutions are Likely to Harm Ordinary Investors*, 14 FORDHAM J. CORP. & FIN. L. 325 (2009) (arguing that smaller companies are particularly prone to under-invest resources in their internal controls over financial reporting).

[1884] SOX § 404(c). *See supra*.

[1885] Udi Hoitash et al., *Corporate Governance and Internal Control over Financial Reporting: A Comparison of Regulatory Regimes*, 84 ACCT. REV. 839, 842 (2009) (stating that their findings suggest "that in regulatory environments without requirements of mandatory testing and independent auditor attestation that are required under Section 404, corporate governance quality has no observable association with ICFR disclosure"). *Cf.* Robert Prentice, *Sarbanes-Oxley: The Evidence Regarding the Impact of SOX 404*, 29 CARDOZO L. REV. 703, 718 (2007).

[1886] 2006 O.J. (L 157) 87 (EC) as amended by Parliament and Council Directive 2008/30, 2008 O.J. (L 81) 53 (EC). The Statutory Audit Directive repealed Council Directive 84/253, 1984 O.J. (L 126) 20 (EEC).

[1887] Sometimes also referred to as the Eighth Company Law Directive.

addresses similar issues as SOX, it is sometimes referred to as "EuroSOX."[1889] However, as the following discussion will show, this name is misleading since it suggests a degree of similarity between SOX and the Statutory Audit Directive that is indeed absent, in particular regarding requirements to disclose an assessment of the effectiveness of an internal control system.

The Statutory Audit Directive's only provision that addresses a company's internal control system is article 41. First, this provision requires "public-interest entities"[1890] (in particular publicly traded companies) to have an audit committee.[1891] The duties of an audit committee include "monitor[ing] the effectiveness of the company's internal control, internal audit where applicable, and risk management systems."[1892]

Second, article 41 provides that the company's "statutory auditor"[1893] or "audit firm"[1894] has to report to the audit committee "on key matters arising from the statutory audit, and in particular on material weaknesses in internal control in relation to the financial reporting

[1888] *See* Statutory Audit Directive recital 5. *Cf. id.* art. 2(1) (defining "statutory audit" as "an audit of annual accounts or consolidated accounts insofar as required by Community law").

[1889] *Cf.* Guido Sanchidrian, *EuroSOX is not US-SOX*, SYMANTEC CONNECT, Mar. 19, 2009, *available at* http://www.symantec.com/connect/articles/eurosox-not-us-sox (noting that the term "EuroSOX" is used in particular by vendors in an effort to sell their products and services).

[1890] *See* Statutory Audit Directive art. 2(13) (defining "public-interest entities" as "entities governed by the law of a Member State whose transferable securities are admitted to trading on a regulated market of any Member State […], credit institutions as defined in point 1 of Article 1 of Directive 2000/12/EC […] and insurance undertakings within the meaning of Article 2(1) of Directive 91/674/EEC").

[1891] *See* Statutory Audit Directive art. 41(1). "At least one member of the audit committee shall be independent and shall have competence in accounting and/or auditing." *Id.*

[1892] *See* Statutory Audit Directive art. 41(2)(b).

[1893] *See* Statutory Audit Directive art. 2(2) (defining "statutory auditor" as "a natural person who is approved in accordance with this Directive by the competent authorities of a Member State to carry out statutory audits").

[1894] *See* Statutory Audit Directive art. 2(3) (defining "audit firm" as "a legal person or any other entity, regardless of its legal form, that is approved in accordance with this Directive by the competent authorities of a Member State to carry out statutory audits").

process."[1895] When performing a statutory audit, statutory auditors and audit firms have to comply with "international auditing standards"[1896] if adopted by the Commission.[1897] However, such standards that may in particular provide further guidance on what constitutes a "material weakness"[1898] have not yet been adopted.[1899]

It has to be emphasized that the Statutory Audit Directive only addresses the reporting of material weaknesses *to the audit committee* but does not address the question of whether information about the internal control system is to be disclosed to the public.

[1895] *See* Statutory Audit Directive art. 41(4).

[1896] *See* Statutory Audit Directive art. 2(11) (defining "international auditing standards" as "International Standards on Auditing (ISA) and related Statements and Standards, insofar as relevant to the statutory audit").

[1897] *See* Statutory Audit Directive art. 26(1). The regulatory procedure with scrutiny is to be used. *See id.* (referring to art. 48(2a) which in turn refers to "Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC […] having regard to the provisions of Article 8 thereof"). The committee that is to assist the Commission for the purpose of adopting international auditing standards is commonly referred to as the "Audit Regulatory Committee."

[1898] *See* INT'L AUDITING & ASSURANCE STANDARDS BD., COMMUNICATING DEFICIENCIES IN INTERNAL CONTROL TO THOSE CHARGED WITH GOVERNANCE AND MANAGEMENT, INTERNATIONAL STANDARD ON AUDITING 265 § 6(b) (2009), *available at* http://web.ifac.org/download/a015-2010-iaasb-handbook-isa-265.pdf (defining "significant deficiency in internal control" as "[a] deficiency or combination of deficiencies in internal control that, in the auditor's professional judgment, is of sufficient importance to merit the attention of those charged with governance"). *See also id.* § A5 (providing examples of factors that the auditor may consider in determining whether deficiency is indeed significant).

[1899] In June 2009, the Commission opened a consultation to seek comments on the possible adoption of the International Standards on Auditing (ISAs) of the International Auditing and Assurance Standards Board (IAASB). DIRECTORATE GEN. FOR INTERNAL MKT. AND SERVS., CONSULTATION ON THE ADOPTION OF INTERNATIONAL STANDARDS ON AUDITING (2009), *available at* http://ec.europa.eu/internal_market/consultations/docs/2009/isa/consultation_ISAs_en.doc. An "overwhelming majority of respondents" stated that they would favor an adoption of the ISAs. DIRECTORATE GEN. FOR INTERNAL MKT. AND SERVS., SUMMARY OF COMMENTS: CONSULTATION ON THE ADOPTION OF THE INTERNATIONAL STANDARDS ON AUDITING 2 (2010), *available at* http://ec.europa.eu/internal_market/auditing/docs/isa/isa-final_en.pdf. *Cf. also* ANNETTE KÖHLER ET AL., EVALUATION OF THE POSSIBLE ADOPTION OF INTERNATIONAL STANDARDS ON AUDITING (ISAS) IN THE EU (2009), *available at* http://ec.europa.eu/internal_market/auditing/docs/ias/study2009/report_en.pdf; ANN VANSTRAELEN ET AL., MAASTRICHT ACCOUNTING, AUDITING AND INFORMATION MANAGEMENT RESEARCH CENTER, EVALUATION OF THE DIFFERENCES BETWEEN INTERNATIONAL STANDARDS ON AUDITING (ISA) AND THE STANDARDS OF THE US PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB) (2009), *available at* http://ec.europa.eu/internal_market/auditing/docs/ias/evalstudy2009/report_en.pdf.

This is the subject of the Fourth Company Law Directive[1900] which, as discussed *supra* in chapter 4.2.2, requires companies whose securities are admitted to trading on a "regulated market"[1901] to include in their annual reports "a description of the main features of the company's internal control and risk management systems in relation to the financial reporting process."[1902] However, the term "main features" cannot be construed to encompass an assessment of the internal control's effectiveness or even its "material weaknesses."

Accordingly, neither the Statutory Audit Directive nor the Fourth Company Law Directive requires the public disclosure of vulnerabilities that could result in the loss of the integrity of information contained in financial reports.

6.1.3. Comparative Assessment

Risks to the integrity of information contained in financial reports issued by publicly traded companies have two important characteristics: (1) they are not transparent to (potential) shareholders and (2) they are primarily born by (potential) shareholders. The first directly relates to the fundamental information security challenge of uninformed risk decisions[1903]: by buying or selling shares, shareholders may make risk decisions without having all relevant information about the integrity risks of reported information. The second characteristic

[1900] Council Directive 78/660, 1978 O.J. (L 222) 11 (EEC) as amended.

[1901] Fourth Company Law Directive art. 46a refers to art. 4(1)(14) of Parliament and Council Directive 2004/39, 2004 O.J. (L 145) 1 (EC) as amended (defining "regulated market" as "a multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments – in the system and in accordance with its non-discretionary rules – in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is authorised and functions regularly and in accordance with the provisions of Title III [of Directive 2004/39]").

[1902] Fourth Company Law Directive art. 46a(1)(c).

[1903] *See supra* chapter 2.4.3.

concerns the challenge of the misalignment between risk and risk mitigation capability[1904]: while a company is the only entity that can mitigate risks to the integrity of its reported financial information, shareholders will suffer most, should the risks materialize.

To not only enable more informed risk decisions but to also create an indirect risk transfer, a disclosure regime has to function as a targeted transparency policy[1905] by ensuring that the disclosed information becomes "embedded"[1906] into the decision-making processes of (potential) shareholders. Such an embeddedness is indeed very likely given that the information is highly relevant, reasonably timely, designed for comparability, and typically interpreted by intermediaries such as brokers or analysts.[1907] By enabling shareholders to make more informed buying or selling decisions, their risks are reduced while, at the same time, the publicly traded companies' risks are increased that a low effectiveness of internal controls will result in a lower stock price. Thus, a disclosure regime can effectively transfer some of the risks associated with financial reporting from the shareholders to the public companies, thereby better aligning risk and risk mitigation capability.

A regulatory regime that seeks to create transparency with regard to the effectiveness of a public company's internal control system has the potential to address both of the challenges outlined above if it ensures (1) that relevant information is disclosed to the public and (2) that the disclosed information is indeed accurate.

[1904] *See supra* chapter 2.4.4.

[1905] *See supra* chapter 3.2.3.2 (describing the basic elements of a targeted transparency policy).

[1906] *See* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 54 (2007).

[1907] *Cf. id.* at 62 (discussing the high "embeddedness" of corporate financial reports in general). *Cf. also* Catherine Shakespeare, *Sarbanes-Oxley Act of 2002 Five Years on: What Have We Learned?*, 3 J. BUS. & TECH. L. 333, 346 (2008) (discussing the mixed results of empirical studies on market reactions to the disclosure of internal control problems).

As regards the first element, SOX requires the disclosure of information regarding the effectiveness of "disclosure controls and procedures" under SOX § 302 and the effectiveness and material weaknesses of "internal control over financial reporting" under SOX § 404. In comparison, the Fourth Company Law Directive only requires the disclosure of the "main features" but not of the effectiveness of the "internal control and risk management systems in relation to the financial reporting process." The information to be disclosed under EU law is much less relevant for shareholders because the features of a control system say little about its effectiveness.

The second element of ensuring that the reported internal control information is indeed accurate is best implemented by mandating an independent audit.[1908] Without such a requirement, a self-assessment would likely fail to discover and/or disclose material weaknesses and would generally overstate the effectiveness of an internal control system.[1909] SOX § 404(b) provides the strong requirement of a mandatory audit by a registered public accounting firm. This requirement is, however, not only limited to "internal control over financial reporting" but also only applies to accelerated filers and large accelerated filers. All other issuers are therefore free to perform a self-assessment. In similarity to SOX § 404(b), the Statutory Audit Directive mandates that a statutory auditor or audit firm report to an

[1908] It has been argued that control-plus-audit programs would generally create the risk to "encourage creation of controls than can be tested rather than controls more likely to be effective." Lawrence A. Cunningham, *The Appeal and Limits of Internal Controls to Fight Fraud, Terrorism, Other Ills*, 29 J. CORP. L. 267, 290 (2004). However, at least regarding internal control over financial reporting, it seems unlikely that not performing any tests would lead to a selection of more effective controls.

[1909] Empirical evidence suggests that the requirement of an independent audit is central to an effective disclosure regime. *See* Udi Hoitash et al., *Corporate Governance and Internal Control over Financial Reporting: A Comparison of Regulatory Regimes*, 84 ACCT. REV. 839, 842 (2009) (stating that their findings suggest "that in regulatory environments without requirements of mandatory testing and independent auditor attestation that are required under Section 404, corporate governance quality has no observable association with ICFR disclosure"). *Cf.* Robert Prentice, *Sarbanes-Oxley: The Evidence Regarding the Impact of SOX 404*, 29 CARDOZO L. REV. 703, 718 (2007).

auditor committee in particular “material weaknesses in internal control in relation to the financial reporting process.” While the Statutory Audit Directive allows Member States to exempt certain types of public-interest entities from this requirement, it does not contain a general exemption for small entities.

In summary, SOX provides both elements—mandatory public disclosure of *relevant* information and ensuring *accuracy* of that information—at least as far as accelerated filers and large accelerated filers are concerned. EU law, however, fails to mandate the disclosure of relevant information and therefore does not have effects comparable to those of SOX § 404.

6.2. Mandatory Data Security Breach Notification

Data security breach notification, also known as “data breach notification,” refers to the regulatory policy of mandating the notification of breaches of the security of personal information to the individuals concerned and/or to third parties such as a government agency. The purpose of a data security breach notification regime can be three-fold: (1) performing an indirect risk transfer by mandating targeted transparency;[1910] (2) performing indirect risk mitigation by mandating notification as a detective security control that allows the individuals concerned to take reactive measures;[1911] or (3) performing indirect risk mitigation enabling deterrent measures by law enforcement agencies.[1912]

[1910] *See supra* chapter 3.2.3.2.

[1911] *See supra* chapter 3.2.1.2 (describing indirect risk mitigation). *Cf. also supra* chapter 3.1 (defining detective and reactive security controls).

[1912] *Cf. supra* chapter 3.2.1.2.

6.2.1. California Senate Bill 1386

In an effort to fight "identity theft,"[1913] California Senate Bill 1386[1914] (codified at California Civil Code §§ 1798.29, 1798.82, and 1798.84) introduced the first breach notification regime in the U.S. It subsequently became a template for breach notification laws passed in many other states.[1915]

California Civil Code § 1798.29 applies to state "agencies"[1916] while the identically worded § 1798.82 applies to "[a]ny person or business that conducts business in California."[1917] Both sections only apply if the entity "owns or licenses computerized data that includes personal information."[1918]

Such entities are required to disclose any "breach of the security of the system" following discovery or notification of the breach to any resident of California[1919] whose unencrypted[1920]

[1913] *See* chapter 4.1.10.1 (discussing the architecture of "identity theft" and why the term "impersonation fraud" better describes the nature of the threat).

[1914] 2002 Cal. Adv. Legis. Serv. 915 (Deering).

[1915] *See* ANNE P. CAIOLA ET AL., U.S. DATA BREACH NOTIFICATION LAW: STATE BY STATE 1 (John P. Hutchins ed., 2007); John B. Kennedy, *Slouching Towards Security Standards: The Legacy Of California's SB 1386*, 865 PLI/PAT 91, 101 (2006).

[1916] *See* CAL. CIV. CODE § 1798.3(b) (West 2010) (defining "agency" as "every state office, officer, department, division, bureau, board, commission, or other state agency, except that the term agency shall not include: (1) The California Legislature. (2) Any agency established under Article VI of the California Constitution. (3) The State Compensation Insurance Fund, except as to any records which contain personal information about the employees of the State Compensation Insurance Fund. (4) A local agency, as defined in subdivision (a) of Section 6252 of the Government Code").

[1917] This does not only include businesses established in California but also businesses that are "selling products or providing services to residents of California." *See* Kevin Poulsen, *California disclosure law has national reach*, SECURITYFOCUS, Jan. 6, 2003, http://www.securityfocus.com/news/1984 (quoting Scott Pink, deputy chair of the American Bar Association's Cybersecurity Task Force).

[1918] *See* CAL. CIV. CODE §§ 1798.29(a), 1798.82(a) (West 2010).

[1919] Accordingly, CAL. CIV. CODE § 1798.82 also applies if a covered entity suffers from a breach that affects only a single California resident. *Cf.* Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 HOUS. L. REV. 1597, 1623 (2007) (noting that the statute gives no guidance regarding how businesses should determine whether a given individual is a California resident).

"personal information" was, or is reasonably believed to have been, acquired[1921] by an unauthorized person.[1922]

An important factor, limiting the material scope of application is the definition of the term "personal information": it only includes "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted"[1923]: (1) Social Security number; (2) driver's license number or California Identification Card number; (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) medical information;[1924] or (5) health insurance information.[1925] "Personal information" does not include "publicly available

[1920] The statute fails to recognize that the use of encryption does not by itself result in a high level of trust in the encrypted data's confidentiality. The security value of an encryption depends, *inter alia,* on the strength of the encryption algorithm, its implementation, the quality (i.e. complexity) of the decryption key, and the current state of technology that is available for trying to break the encryption, e.g., by means of a brute force attack or a dictionary attack. *Cf.* Joost Houwen, *Methods of Attacking and Defending Cryptosystems, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1255 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007). *See also* Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet A Suitable Template For National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, 11 (2003), *available at* http://jolt.richmond.edu/v10i1/article1.pdf (criticizing the encryption exemption as too vague).

[1921] *Cf.* Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet A Suitable Template For National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, 8 (2003), *available at* http://jolt.richmond.edu/v10i1/article1.pdf (criticizing the "reasonable belief of acquisition"-standard as too vague and stating that "mere access to data, not actual theft or use of the information will trigger [the notification obligation]").

[1922] *See* CAL. CIV. CODE §§ 1798.29(a), 1798.82(a).

[1923] *See* CAL. CIV. CODE §§ 1798.29(e), 1798.82(e).

[1924] *See* CAL. CIV. CODE §§ 1798.29(f)(2), 1798.82(f)(2) (defining "medical information" as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional"). CAL. CIV. CODE §§ 1798.29(e), 1798.82(e) were amended to also include medical information by A.B. 1298, 2007 Cal. Legis. Serv. Ch. 699 (West).

[1925] *See* CAL. CIV. CODE §§ 1798.29(f)(3), 1798.82(f)(3) (defining "health insurance information" as "an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records"). CAL. CIV. CODE §§ 1798.29(e), 1798.82(e) were amended to also include health insurance information by A.B. 1298, 2007 Cal. Legis. Serv. Ch. 699 (West).

information that is lawfully made available to the general public from federal, state, or local government records."[1926]

Equally important, "breach of the security of the system" is defined as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the [covered entity]."[1927]

While clearly excluding non-computerized data[1928] from the material scope of application, this definition also raises a number of questions: First, what is the meaning of the enumeration "security, confidentiality, or integrity"—given that "security" is traditionally defined as encompassing the latter two?[1929] Second, how can the acquisition of data compromise its integrity?[1930] Since the plain language of the statute only covers an "unauthorized acquisition" but not data destruction, corruption, or modification, §§ 1798.29, 1798.82 have to be construed as only covering the compromise of confidentiality but not the compromise of any other property of information security (i.e. integrity or availability).[1931]

[1926] *See* CAL. CIV. CODE §§ 1798.29(f)(1), 1798.82(f)(1).

[1927] *See* CAL. CIV. CODE §§ 1798.29(d), 1798.82(d).

[1928] *See* Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet A Suitable Template For National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, 10 (2003), *available at* http://jolt.richmond.edu/v10i1/article1.pdf (criticizing the exclusion of paper records the disclosure of which can be equally damaging to individuals).

[1929] *See supra* chapter 2.1 (defining information security and providing further references).

[1930] *Cf.* ISO & IEC, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, ISO/IEC 27000:2009 § 2.25 (2009) (defining "integrity" as "property of protecting the accuracy and completeness of assets").

[1931] The same conclusion can also be reached by considering that Senate Bill 1386 is primarily concerned about "identity theft"—a crime that requires the perpetrator to acquire (and not to destroy, corrupt, or modify) identifying information. *See* California Senate Bill 1386 § 1(e) (stating that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative").

However, not every compromise of confidentiality constitutes a "breach of the security of the system." The acquisition of personal information by an employee or an agent of the covered entity does not constitute a breach if: (1) the acquisition is performed in good faith and for the purposes of the covered entity; and (2) the personal information is neither subsequently used nor subject to further unauthorized disclosure.[1932]

Regarding the method of notification to individuals, the statute provides that a covered entity many choose between a "written notice" and an "electronic notice."[1933] The latter has to be consistent with the federal Electronic Signatures in Global and National Commerce Act (E-SIGN)[1934] which requires prior consent to electronic notice.[1935]

The statute also allows for a "substitute notice" if the covered entity demonstrates (1) that the cost of providing notice would exceed $250,000; (2) that more than 500,000 individuals would have to be notified; or (3) that the covered entity does not have sufficient contact information.[1936] A substitute notice consists of all of the following: (a) e-mail notice when the covered entity has the individuals' e-mail addresses; (b) conspicuous posting of the notice on the entity's "Web site page,"[1937] if the entity maintains one; and (c) notification to major statewide media.[1938]

[1932] CAL. CIV. CODE §§ 1798.29(d), 1798.82(d).

[1933] CAL. CIV. CODE §§ 1798.29(g), 1798.82(g).

[1934] Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified at 15 U.S.C. § 7001 et seq.).

[1935] CAL. CIV. CODE §§ 1798.29(g)(2), 1798.82(g)(2). *See* 15 U.S.C. § 7001(c)(1)(A) (requiring that "the consumer has affirmatively consented to such use and has not withdrawn such consent").

[1936] *See* CAL. CIV. CODE §§ 1798.29(g)(3), 1798.82(g)(3).

[1937] Whether this refers to the website's homepage is unclear.

[1938] *See* CAL. CIV. CODE §§ 1798.29(g)(3)(A)-(C), 1798.82(g)(3)(A)-(C).

Regarding the timeliness of notification, the statute provides that individuals have to be notified “in the most expedient time possible and without unreasonable delay.” However, notifications may be delayed “if a law enforcement agency determines that the notification will impede a criminal investigation.”[1939] Furthermore, the timing has to be “consistent with […] any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.”[1940]

It should be noted, that the plain language of the statute does not require any specific information items to be included in a notification.[1941] This not only reduces the value a notification has to the individuals who receive it but also limits the amount of transparency created by the notification regime.

It should be stressed that §§ 1798.29, 1798.82 do not only provide obligations for an entity that “owns or licenses” data but also for an entity that “maintains”[1942] data: a covered entity that “maintains computerized data that includes personal information that the [entity] does not own” has to notify the information’s “owner or licensee” of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[1943]

[1939] CAL. CIV. CODE §§ 1798.29(c), 1798.82(c).

[1940] CAL. CIV. CODE §§ 1798.29(a), 1798.82(a).

[1941] California Senate Bill 20, 2009 Leg. (Cal. 2009) which would have prescribed a minimum content for notifications was vetoed by the Governor of California on Oct. 11, 2009. Senate Bill 20 was reintroduced in 2010 as Senate Bill 1166, 2009 Leg. (Cal. 2009) which was also vetoed by the Governor on Sept. 29, 2010.

[1942] *See* CAL. CIV. CODE § 1798.3(e) (stating that “the term ‘maintain’ includes maintain, acquire, use, or disclose”).

[1943] CAL. CIV. CODE §§ 1798.29(b), 1798.82(b).

The notification requirements are subject to private and public enforcement: A "customer" who has been injured by a violation of §§ 1798.29, 1798.82 may institute a civil action to recover damages.[1944] Furthermore, a business that violates, proposes to violate, or has violated its obligations may also be enjoined.[1945] Since a violation of § 1798.82 constitutes an act of unfair competition,[1946] the attorney general may also bring an action for an injunction[1947] or for civil penalties.[1948]

6.2.2. California Senate Bill 541

California Senate Bill 541[1949] was passed in 2008 and added § 1280.15 to the California Health and Safety Code. § 1280.15(b) creates an obligation for all clinics, health facilities, home health agencies, and licensed hospices[1950] to report any "unlawful or unauthorized access to, or use or disclosure of,"[1951] a patient's "medical information" to the California Department of Public Health (hereinafter *CDPH*) as well as the affected patients.

[1944] CAL. CIV. CODE § 1798.84(b). By using the undefined term "customer," the statute seems to exclude civil actions against all covered entities with which the plaintiff does not have a customer relationship with, e.g., the State of California, employers, and data brokers. *See* Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet A Suitable Template For National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, 40 (2003), *available at* http://jolt.richmond.edu/v10i1/article1.pdf (noting the irony of this deficiency: it was a breach of employee information in a California state database that caused the bill to be passed in the first place).

[1945] CAL. CIV. CODE § 1798.84(e).

[1946] *See* CAL. BUS. & PROF. CODE § 17200 (stating that "unfair competition" shall include "any unlawful […] business act or practice").

[1947] *See* CAL. BUS. & PROF. CODE § 17204.

[1948] *See* CAL. BUS. & PROF. CODE § 17206.

[1949] 2008 Cal. Legis. Serv. Ch. 605 (West).

[1950] CAL. HEALTH & SAFETY CODE § 1280.15(b) (West 2010) only covers hospices that are licensed pursuant to CAL. HEALTH & SAFETY CODE §§ 1204, 1250, 1725, or 1745.

[1951] *See* CAL. HEALTH & SAFETY CODE § 1280.15(j)(2) (defining "unauthorized" as "the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act (Part 2.6 (commencing with

To define "medical information," the statute refers to California Civil Code § 56.05(g) which provides that the term is to be understood as any "individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment."[1952]

Since the statute only refers to "unauthorized access," "use," and "disclosure"[1953]—but not to other acts such as alteration or destruction—it only covers security breaches that compromise the confidentiality of medical information. Breaches that only compromise the integrity or availability therefore do not have to be notified under Senate Bill 541.

Covered breaches have to be notified to the CDPH as well as to the affected patients (or their representatives) no later than five business days after they have been detected.[1954] In 2009, California Senate Bill 337[1955] amended the statute to allow the postponement of breach notification for the purpose of preventing compromise of a law enforcement criminal investigation.[1956] However, only the notification of the affected patients but not the notification of the CDPH may be postponed.[1957] Furthermore, a delayed patient notification is

Section 56) of Division 1 of the Civil Code) or any other statute or regulation governing the lawful access, use, or disclosure of medical information").

[1952] CAL. CIV. CODE § 56.05(g). "Individually identifiable" is defined as including or containing "any element of personal identifying information sufficient to allow identification of the individual […] or other information that, alone or in combination with other publicly available information, reveals the individual's identity." *Id.*

[1953] *See* CAL. HEALTH & SAFETY CODE § 1280.15(b)(1) and (2).

[1954] *See id.*

[1955] 2009 Cal. Legis. Serv. Ch. 180 (West).

[1956] *Cf.* Thomas J. Smedinghoff & Stephen S. Wu, *State Security Laws And Regulations—The New Deal*, 969 PLI/PAT 365, 378 (2009) (noting this deficiency before Senate Bill 337 was adopted).

[1957] *See* CAL. HEALTH & SAFETY CODE § 1280.15(c)(1) (only referring to "the reporting, as required pursuant to paragraph (2) of subdivision (b)" but not to the reporting to the CDPH under § 1280.15(2)(a)).

only permissible when a law enforcement agency or official provides a written statement or a (subsequently documented)[1958] oral statement that a notification of the patients would be "likely to impede the law enforcement agency's activities that relate to [the breach]."[1959] Such a statement also has to specify the duration of the delay which may not exceed 60 days in case of a written statement and not 30 days in case of an oral statement.[1960] Based on a subsequent written request from a law enforcement agency or official, the delay may be extended for another 60 days.[1961]

As regards the method of notification, § 1280.15(b)(2) provides that patients have to be notified "at the last known address." In contrast to Senate Bill 1386 discussed *supra*,[1962] Senate Bill 541 therefore only allows notifications of patients to be sent individually by regular mail. However, the method of notification of the CDPH is left unspecified by the statute.

Regarding the content of a breach notification, Senate Bill 541 did not introduce any provisions that would make the inclusion of any particular information mandatory.[1963]

Pursuant to California Health and Safety Code § 1280.15(d), the CDPH may sanction violations of the notification obligations with a penalty in the amount of $100 per day of

[1958] *See* CAL. HEALTH & SAFETY CODE § 1280.15(c)(2)(A) (stating that the clinic, health facility, home health agency, or hospice has to "[d]ocument the oral statement, including, but not limited to, the identity of the law enforcement agency or official making the oral statement and the date upon which the oral statement was made").

[1959] *Id.*

[1960] *See id.*

[1961] This requires a written declaration from the law enforcement agency that there exists "a bona fide, ongoing, significant criminal investigation of serious wrongdoing relating to the [breach], that notification of patients will undermine the law enforcement agency's activities, and that specifies a date upon which the delay shall end." *Id.*

[1962] *See supra* chapter 6.2.1.

[1963] This resembles the approach taken by Senate Bill 1386. *See id.*

delayed notification of a breach.[1964] However, the total combined penalty for a violation of the notification obligation under § 1280.15(b) and the obligation to prevent breaches under § 1280.15(a)[1965] may not exceed $250,000 per "reported event." This wording raises the question of whether there is a maximum in cases in which the breach is never reported. § 1280.15(j)(2) defines the term "reported event" as "all breaches included in any single report that is made pursuant to subdivision (b), regardless of the number of breach events contained in the report."[1966] This makes clear that the purpose of the liability cap is to limit the financial disincentive for reporting breaches. However, if a breach is not reported, the $250,000 cap for a "reported event" does not apply.[1967]

6.2.3. The New York Information Security Breach and Notification Act

In 2005, New York enacted the Information Security Breach and Notification Act (ISBNA).[1968] It added New York General Business Law § 899-aa which applies to "[a]ny person or business which conducts business in New York state" and the almost identically worded New York State Technology Law § 208 which covers any "state entity."[1969]

[1964] *See* CAL. HEALTH & SAFETY CODE § 1280.15(d). A summary by county of penalties assessed by the CDPH is available at http://www.cdph.ca.gov/certlic/facilities/Pages/Counties.aspx (last accessed Feb. 10, 2011).

[1965] *See supra* chapter 5.1.5.4.

[1966] CAL. HEALTH & SAFETY CODE § 1280.15(j)(2).

[1967] *But see* Thomas J. Smedinghoff & Stephen S. Wu, *State Security Laws And Regulations—The New Deal*, 969 PLI/PAT 365, 378 (2009) (apparently not making this distinction).

[1968] Information Security Breach and Notification Act, 2005 N.Y. Sess. Laws Ch. 442 (McKinney) (codified at N.Y. STATE TECH. LAW § 208 and N.Y. GEN. BUS. LAW § 899-aa). *Cf. generally* ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE § 25:207 (2009); ANNE P. CAIOLA ET AL., U.S. DATA BREACH NOTIFICATION LAW: STATE BY STATE 54 (John P. Hutchins ed., 2007). Note that this law largely preempts the corresponding New York City law, N.Y.C. CODE § 20-117, which will not be discussed here. *See id.* at 57.

[1969] *See* N.Y. STATE TECH. LAW § 208(1)(c) (McKinney 2010) (defining "state entity" as "any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, The basic provisions that mandate the notification of the individuals concerned closely resemble California Civil Code §§ 1798.29, 1798.82. An entity covered by New York State Technology Law § 208 or New York General Business Law § 899-aa, if it "owns or licenses computerized data which includes private information," has to disclose any "breach of the security of the system" to any resident of New York state "whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization."[1970]

The term "private information" as it is used in ISBNA[1971] differs only in two respects from the term "personal information" as it is used in California Civil Code §§ 1798.29, 1798.82: (1) it neither includes medical information nor health insurance information; and (2) it provides that information "encrypted with an encryption key that has also been acquired" is to be treated as "not encrypted."[1972] Like under the California law, "publicly available information […] lawfully made available to the general public from federal, state, or local government records" is not covered.[1973]

office or other governmental entity performing a governmental or proprietary function for the state of New York, except: (1) the judiciary; and (2) all cities, counties, municipalities, villages, towns, and other local agencies").

[1970] *See* N.Y. STATE TECH. LAW § 208(2), N.Y. GEN. BUS. LAW § 899-aa(2).

[1971] *See* N.Y. STATE TECH. LAW § 208(1)(a), N.Y. GEN. BUS. LAW § 899-aa(1)(b) (defining "private information" as "personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account").

[1972] *Id.* Note that this wording focuses on symmetric cryptographic algorithms which use the same key for encryption as well as for decryption. If an asymmetric cryptographic algorithm is used, the confidentiality of the encryption key is of no relevance. *Cf.* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 4 (2d ed. 1996).

[1973] *See* N.Y. STATE TECH. LAW § 208(1)(a), N.Y. GEN. BUS. LAW § 899-aa(1)(b).

ISBNA also provides the same definition for the term "breach of the security of the system" as does California Civil Code §§ 1798.29, 1798.82.[1974] However, it additionally enumerates factors a covered entity "may consider […] among others" in determining whether information has been acquired, or is reasonably believed to have been acquired without valid authorization: (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of "identity theft" reported.[1975]

The ISBNA's timeliness requirements are identical to California Civil Code §§ 1798.29, 1798.82.[1976] The requirements regarding the method of notification, however, differ:

Electronic notice is only permissible if: (1) the individual "expressly consented to receiving said notice in electronic form"; (2) a log of each notification is kept; and (3) consent to accepting the electronic notice was not a condition for establishing the business relationship or engaging in the transaction.[1977]

[1974] *See* N.Y. STATE TECH. LAW § 208(1)(b), N.Y. GEN. BUS. LAW § 899-aa(1)(c) (defining "breach of the security of the system" as "unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a [covered entity]"). The N.Y. statute also provides an identical exception for good faith acquisitions by employees or agents of the covered entity. *See id.*

[1975] N.Y. STATE TECH. LAW § 208(1)(b), N.Y. GEN. BUS. LAW § 899-aa(1)(c).

[1976] Notice must be given "in the most expedient time possible and without unreasonable delay" but only *after* a law enforcement agency determines that the notification does not compromise a criminal investigation and only if the notification is "consistent with […] any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system." *See* N.Y. STATE TECH. LAW § 208(2) and (4), N.Y. GEN. BUS. LAW § 899-aa(2) and (4).

[1977] *See* N.Y. STATE TECH. LAW § 208(5)(b), N.Y. GEN. BUS. LAW § 899-aa(5)(b).

In addition to a written notice or an electronic notice, ISBNA also allows for a "telephone notification" provided that "a log of each such notification is kept" by the covered entity.[1978] The requirements and form of a substitute notice, on the other hand, are identical to California Civil Code §§ 1798.29, 1798.82.[1979]

In contrast to the California statute, ISBNA also defines the minimum content of a notification: (1) contact information for the covered entity making the notification and (2) a description of the categories of information that were, or are reasonably believed to have been, acquired without valid authorization. Accordingly, a notification does not have to state the cause of the breach or the number of individuals affected.

Another major difference to the California statute is that ISBNA also requires the notification of third parties: if a covered entity has to notify a New York resident, it must also notify: (1) the state Attorney General,[1980] (2) the Consumer Protection Board,[1981] and (3) the state Office of Cyber Security and Critical Infrastructure Coordination[1982] (CSCIC).[1983] The notice to these third parties has to include information about "the timing, content and distribution of the notices and approximate number of affected persons."[1984] If more than 5,000 New York

[1978] *See* N.Y. STATE TECH. LAW § 208(5)(c), N.Y. GEN. BUS. LAW § 899-aa(5)(c).

[1979] *See* N.Y. STATE TECH. LAW § 208(5)(d), N.Y. GEN. BUS. LAW § 899-aa(5)(d).

[1980] *Cf.* http://www.ag.ny.gov/bureaus/consumer_frauds/tips/id_theft_law.html (last accessed Feb. 10, 2011).

[1981] *Cf.* http://www.consumer.state.ny.us/business_interests/manage_sb.htm (last accessed Feb. 10, 2011).

[1982] *Cf.* http://www.cscic.state.ny.us/security/securitybreach (last accessed Feb. 10, 2011).

[1983] *See* N.Y. STATE TECH. LAW § 208(7)(a), N.Y. GEN. BUS. LAW § 899-aa(8)(a).

[1984] *Id.*

residents are to be notified at one time, a covered entity must also provide this information in a notice to "consumer reporting agencies."[1985]

Identical to California Civil Code §§ 1798.29, 1798.82, ISBNA also mandates that covered entities that maintain but do not own computerized private information immediately notify the owner or licensee of the information of any security breach,[1986] which in turn puts the owner/licensee under an obligation to notify the individuals concerned.

New York General Business Law § 899-aa is to be enforced by the state's attorney general. He may bring an action in the name and on behalf of the people to enjoin and restrain the continuation of a violation.[1987] In such action, the court may award damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses.[1988] If the business violated § 899-aa knowingly or recklessly, the court may impose a civil penalty of the greater of $5,000 or up to $10 per instance of failed notification, provided that the latter amount shall not exceed $150,000.[1989] New York State Technology Law § 208 does not provide an enforcement mechanism.

[1985] *See* N.Y. STATE TECH. LAW § 208(7)(b), N.Y. GEN. BUS. LAW § 899-aa(8)(b). *Cf.* N.Y. STATE TECH. LAW § 208(1)(b), N.Y. GEN. BUS. LAW § 899-aa(1)(d) (defining "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports").

[1986] *See* N.Y. STATE TECH. LAW § 208(3), N.Y. GEN. BUS. LAW § 899-aa(3).

[1987] *See* N.Y. GEN. BUS. LAW § 899-aa(6)(a).

[1988] *Id.*

[1989] *Id.*

6.2.4. The HITECH Act

Since 2005, data security breach notification requirements have been debated on the federal level. Despite numerous proposals, Congress has not yet passed a comprehensive data security breach notification bill.[1990] The requirements that currently exist under federal law are characterized by a fragmented and mostly sector-specific approach.[1991]

The latest of these sector specific approaches is implemented by the Health Information Technology for Economic and Clinical Health Act (HITECH Act)[1992] which was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA).[1993] The HITECH Act introduced a federal data security breach notification regime for two separate groups of entities: (1) entities covered under HIPAA and their associates; and (2) vendors of personal health records, and other entities not covered by HIPAA. HITECH Act §§ 13402,[1994] 13407[1995] respectively place the first group under the jurisdiction of the Department of Health and Human Services (HHS) and the second under the jurisdiction of the Federal Trade Commission (FTC).

[1990] *Cf.* Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1131 (2009) (assessing the likelihood of passage of a federal data security breach notification bill).

[1991] *See generally* GINA STEVENS, CONG. RESEARCH SERV., FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS, CRS REPORT FOR CONGRESS RL34120 (2010), *available at* http://opencrs.com/document/RL34120/2010-01-28/download/1013.

[1992] Division A, Title XIII and Division B, Title IV of the American Recovery and Reinvestment Act of 2009.

[1993] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009)

[1994] 42 U.S.C. § 17932 (2010).

[1995] 42 U.S.C. § 17937 (2010).

6.2.4.1. The HHS Breach Notification Rule

HITECH Act § 13402 and the HHS Breach Notification Rule[1996] issued pursuant to HITECH Act 13402(j) provide a breach notification regime for health plans, health care clearinghouses, and health care providers ("covered entities")[1997] as well as their business associates.[1998] The breach notification requirements for "covered entities" shall be considered first.

§ 13402(a) requires a covered entity, without unreasonable delay and in no case later than 60 calendar days after discovery[1999] of a "breach" of "unsecured protected health information," to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of [a] breach."

"Protected health information" is defined broadly as "individually identifiable health information […] transmitted or maintained in any […] form or medium."[2000] The breach of such information, however, only results in an obligation to notify in case the information was "unsecured," that is, in case it was not secured through the use of a technology or methodology that renders it "unusable, unreadable, or indecipherable to unauthorized

[1996] Breach Notification for Unsecured Protected Health Information; Interim final rule with request for comments, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 160, 164).

[1997] *See* HITECH Act § 13400(3), 42 U.S.C. § 17921(3) (referring to 45 C.F.R. § 160.103).

[1998] *See* HITECH Act § 13400(2), 42 U.S.C. § 17921(2) (referring to 45 C.F.R. § 160.103).

[1999] *See* HITECH Act § 13402(d), 42 U.S.C. § 17932(d); 45 C.F.R. § 164.404(b). *Cf.* HITECH Act § 13402(c), 42 U.S.C. § 17932(c) (stating that a breach shall be treated as discovered "as of the first day on which such breach is known to such entity […] (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity […]) or should reasonably have been known to such entity […] to have occurred"). *Cf.* 45 C.F.R. § 164.404(2).

[2000] *See* HITECH Act § 13400(12), 42 U.S.C. § 17921(12) (referring to 45 C.F.R. § 160.103). Specifically, this also includes information maintained in paper form. *Cf.* Jason W. Davis, *HITECH HIPAA Amendments: New Rules on Breach Notification, Business Associate Compliance, and Enforcement*, HEALTH LAW., June 2009, at 23, 23.

individuals"[2001] as specified in a guidance issued by the Secretary of HHS.[2002] The guidance refers to media destruction processes[2003] and to encryption processes that comply with standards issued by the National Institute of Standards and Technology (NIST).[2004]

Equally important as the definition of the type of information covered by the provision, is the definition of the term "breach." HITECH Act § 13400(1)(A) defines it as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information." This raises the question whether only breaches of data confidentiality or also of integrity and/or availability are covered.

The first issue is the meaning of "security or privacy." While the latter is left undefined, "security" is defined in HITECH Act § 13400(14) by referring to 45 C.F.R. § 164.304. However, regarding the term "security" by itself, § 164.304 only provides that it encompasses "all of the administrative, physical, and technical safeguards in an information system." More insight can be gained from the fact that 45 C.F.R. § 164.304 defines the term "security incident" as "the attempted or successful unauthorized access, use, disclosure, *modification, or destruction* of information *or interference with system operations* in an information system" (emphasis added). This suggests that the term "security" covers confidentiality,

[2001] HITECH Act § 13402(h)(2), 42 U.S.C. § 17932(h)(2).

[2002] *See* Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, 74 Fed. Reg. 42,740, 42,742 (Aug. 24, 2009) (issued pursuant to HITECH Act § 13402(h)(2)).

[2003] Redaction is specifically excluded as a means of data destruction. Electronic media has to be cleared, purged, or destroyed consistent with NIST, GUIDELINES FOR MEDIA SANITIZATION, SPECIAL PUBLICATION 800-88 (2006), *available at* http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

[2004] The guidance refers to NIST, GUIDELINES FOR THE SELECTION AND USE OF TRANSPORT LAYER SECURITY (TLS) IMPLEMENTATIONS, SPECIAL PUBLICATIONS 800-52 (2005); NIST, GUIDE TO SSL VPNS, SPECIAL PUBLICATION 800-113 (2008); and others which are validated under NIST, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 140—2 (2001). *Cf.* Patrick Nolan, *Unusable, Unreadable, or Indecipherable? No Breach reporting required*, SANS INTERNET STORM CENTER, May 9, 2009, http://isc.sans.org/diary.html?storyid=6364.

integrity, and availability. However, as stated above, HITECH Act § 13400(1)(A) does not define "breach" as any "compromise of security" but rather as "the unauthorized acquisition, access, use, or disclosure" that compromises security. Since HITECH Act § 13400(1)(A) does not use the very terms that are used in 45 C.F.R. § 164.304 to refer to compromises of integrity or availability ("modification," "destruction," and "interference with system operations"), "breach" has to be construed as only covering breaches of confidentiality.

The plain language of this definition does not require the risk of any future harm. The statute only excludes three specific narrowly defined cases in which no harm (and no risk of future harm) is caused by an incident.[2005] However, it has to be emphasized that the HHS Breach Notification Rule adds a general risk-of-harm requirement by defining "compromises the security or privacy of the protected health information" as "poses a significant risk of financial, reputational, or other harm to the individual."[2006] The HHS Breach Notification Rule claims that "[t]his ensures better consistency and alignment with State breach notification laws, as well as existing obligations on Federal agencies (some of which also must comply with these rules as HIPAA covered entities) pursuant to OMB Memorandum M-07-16."[2007] To determine whether a "risk of financial, reputational, or other harm to the

[2005] *See* HITECH Act § 13400(1)(B), 42 U.S.C. § 17921(1)(B) (providing that the term "breach" does not include the following cases: (1) an employee or individual acting under the authority of a covered entity unintentionally acquired, accessed, or used protected health information in good faith and within the course and scope of the employment and such information is not further acquired, accessed, used, or disclosed by any person (*see also* 45 C.F.R. § 164.402(2)(i)); (2) inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility if the information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person (*see also* 45 C.F.R. § 164.402(2)(ii)); and (3) a disclosure where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information (*see also* 45 C.F.R. § 164.402(2)(iii))).

[2006] 45 C.F.R. § 164.402 (2010).

[2007] 74 Fed. Reg. 42,740, 42,744 (Aug. 24, 2009). *Cf. id.* (claiming that the statutory language of the HITECH Act would "encompasses a harm threshold"). *Cf. infra* chapter 6.2.8 (discussing OMB Memorandum M-07-16).

individual" exists that is "significant," a fact-specific risk assessment has to be performed by the covered entity.[2008] However, the disclosure of information that does not include the identifiers listed at 45 C.F.R. § 164.514(e)(2),[2009] date of birth, or zip code never poses a "significant risk."[2010]

Regarding the method of the notice that has to be provided to individuals, HITECH Act § 13402(e)(1) states that, in general, written notification by first-class mail is required. Notification by electronic mail is only sufficient "if specified as a preference by the individual."[2011] If there is insufficient or out-of-date contact information that precludes direct written (or electronic) notice, a substitute form of notice shall be provided that is "reasonably calculated to reach the individual."[2012] If a substitute notice is required for fewer than 10 individuals, it may be provided "by an alternative form of written notice, telephone, or other means."[2013] If, however, a substitute notice is required for 10 or more individuals, a covered entity has to: (1) make a conspicuous posting for 90 days on the home page of its website;[2014] or (2) issue a notice in major print or broadcast media, including major media in geographic

[2008] *Id. Cf.* Andrew B. Wachler & Amy K. Fehn, *The HITECH Breach Notification Rules: Understanding the New Obligations*, HEALTH LAW., Oct. 2009, at 1, 5 (discussing factors that should be considered when performing the risk assessment).

[2009] These identifiers are: names; postal address information, other than town or city, state, and zip code; telephone numbers; fax numbers; electronic mail addresses; Social Security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web universal resource locators (URLs); Internet Protocol address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

[2010] *See* 45 C.F.R. § 164.402(1)(ii).

[2011] *Cf.* 45 C.F.R. § 164.404(d)(1)(i) (stating that electronic notice is only permissible "if the individual agrees to electronic notice and such agreement has not been withdrawn").

[2012] 45 C.F.R. § 164.404(d)(2).

[2013] 45 C.F.R. § 164.404(d)(2)(i).

[2014] 45 C.F.R. § 164.404(d)(2)(ii)(A).

areas where the individuals affected by the breach likely reside.[2015] A notice to 10 or more individuals has to include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may have been affected by the breach.[2016]

The notice has to include, to the extent possible, the following information in "plain language"[2017]: (1) a brief description of what happened; (2) a description of the types of unsecured protected health information that were involved in the breach; (3) the steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.[2018]

In addition to the individuals concerned, the Secretary of HHS also has to be notified of all breaches contemporaneously with the notification provided to individuals.[2019] If less than 500 individuals are affected by the breach, it is sufficient to notify the Secretary on a yearly basis

[2015] *Id.*

[2016] 45 C.F.R. § 164.404(d)(2)(ii)(B).

[2017] *See* 45 C.F.R. § 164.404(c)(2).

[2018] *See* HITECH Act § 13402(f), 42 U.S.C. § 17932(f); 45 C.F.R. § 164.404(c)(1). Note that the HHS Breach Notification Rule does not require the number of affected individuals to be disclosed. However, the electronic form that has to be used to submit breach notifications to the Secretary of HHS does ask for the "Approximate Number of Individuals Affected by the Breach." *See* http://transparency.cit.nih.gov/breach/index.cfm (last accessed Feb. 10, 2011).

[2019] *See* HITECH Act § 13402(e)(3), 42 U.S.C. § 17932(e)(3). *Cf.* 45 C.F.R. § 164.408. The notice must be submitted electronically by filling out an online form. *See* http://transparency.cit.nih.gov/breach/index.cfm (last accessed Feb. 10, 2011).

but not later than 60 days after the end of each calendar year.[2020] The Secretary, in turn, has to publish a list on the HHS's website[2021] that identifies all covered entities involved in a breach in which the unsecured protected health information of more than 500 individuals was acquired or disclosed.[2022] Since neither the statute nor the HHS Breach Notification Rule requires the Secretary to publish any additional information about reported breaches, the usefulness of the list remains rather limited.[2023]

If the unsecured protected health information of more than 500 residents of a State or jurisdiction has been breached, notice also has to be provided to prominent media outlets serving such a State or jurisdiction. The requirements regarding the timeliness and the content of the notification are identical to those applying to the notifications that have to be provided to individuals.[2024]

As stated above, the HITECH Act gives the HHS not only authority over HIPAA "covered entities" but also over their business associates.[2025] HITECH Act § 13402(b) provides that a

[2020] *Id.*

[2021] This list is currently available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html (last accessed Feb. 10, 2011).

[2022] *See* HITECH Act § 13402(e)(3), 42 U.S.C. § 17932(e)(4). *Cf.* 45 C.F.R. § 164.408(c).

[2023] Currently the list contains the following information items: entity name, state, approximate number of individuals affected, date of breach, type of breach (theft, loss, improper disposal, unauthorized access, Hacking/IT incident, other, or unknown), and location of breached information (laptop, desktop computer, network server, e-mail, other portable electronic device, electronic medical record, paper, or other). *See* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html (last accessed Feb. 10, 2011). Other information contained in the notification (i.e. a brief description of the breach, the safeguards in place prior to the breach, whether substitute and/or media notice was required, and actions taken in response to the breach) are not disclosed to the public.

[2024] *See* 45 C.F.R. § 164.406(b) (stating that, except for law enforcement purposes, the notification has to be performed "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach"). *See* 45 C.F.R. § 164.406(c) (stating that the notification provided to the media shall meet the requirements of 45 C.F.R. § 164.404(c)).

[2025] *See* HITECH Act § 13400(2), 42 U.S.C. § 17921(2) (referring to 45 C.F.R. § 160.103). Examples of business associates include third party administrators or pharmacy benefit managers for health plans, claims processing or business associate of a covered entity has to notify the covered entity of all breaches of unsecured protected health information.[2026] The notification has to be performed without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.[2027] The notification has to include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.[2028] Additionally, the notification also has to include any other available information that the covered entity is required to include in notifications to the individuals concerned.[2029] It should be stressed that business associates—unlike HIPPA "covered entities"—do not have to notify the Secretary of HHS, media outlets, or the individuals concerned. However, the business associates' obligation to notify the covered entity serves a very important purpose: it prevents a covered entity from outsourcing data processing operations to business associates in a way that it will not "discover" any breaches.

Violations of the HITECH Act by a covered entity[2030] or a business associate[2031] are subject to enforcement and penalties under Social Security Act §§ 1176, 1177.[2032] The HITECH Act

billing companies, transcription companies, and persons who perform legal, actuarial, accounting, management, or administrative services for covered entities and who require access to protected health information. *See* 74 Fed. Reg. 42,740, 42,740 (Aug. 24, 2009).

[2026] *Cf.* 45 C.F.R. § 164.410(a)(1) (stating that "[a] business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach").

[2027] *See* 45 C.F.R. § 164.410(a)(2) (providing an exception for law enforcement purposes).

[2028] HITECH Act § 13402(b), 42 U.S.C. § 17932(b). *Cf.* 45 C.F.R. § 164.410(c)(1).

[2029] 45 C.F.R. § 164.410(c)(2).

[2030] *See* HITECH Act § 13410(a)(2).

[2031] *See* HITECH Act §§ 13401(b), 13404(c).

[2032] 42 U.S.C. §§ 1320d-5, 1320d-6. *Cf.* Andrew B. Wachler & Amy K. Fehn, *The HITECH Breach Notification Rules: Understanding the New Obligations*, HEALTH LAW., Oct. 2009, at 1, 10.

strengthened the Social Security Act's enforcement mechanisms by providing considerable higher civil penalties,[2033] *parens patriae* actions by State attorneys general,[2034] and a duty of the Secretary of the HHS to investigate and subsequently impose penalties for violations due to willful neglect.[2035] The HHS started to enforce the HHS Breach Notification Rule on February 22, 2010.[2036] In an enforcement action, a covered entity or a business associate has the burden of demonstrating that all notifications were made as required, including evidence demonstrating the necessity of any delay.[2037]

6.2.4.2. The FTC Health Breach Notification Rule

HITECH Act § 13407 introduced a breach notification regime for (1) vendors of personal health records (PHR vendors), (2) PHR related entities, and (3) third party service providers.

[2033] 42 U.S.C. § 1320d-5(a) as amended by American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009), § 13410(d)(2), implements a differentiated approach regarding minimum penalties, distinguishing whether (A) the person who is in violation "did not know (and by exercising reasonable diligence would not have known)" that such person was in violation (at least $100 for each violation); (B) the violation was "due to reasonable cause and not to willful neglect" (at least $1,000 for each violation); or (C) the violation was due to willful neglect (depending on whether the violation was corrected, at least $10,000 or $50,000 for each violation). The maximum penalty for a single violation is $50,000 and for all violations of an identical provision in a calendar year $1,500,000. *Cf.* HITECH Act Enforcement Interim Final Rule, 74 Fed. Reg. 56,123, 56,127 (Oct. 30, 2009).

[2034] The attorney general of a State may bring a civil action to enjoin further violation of the same provision or to obtain damages on behalf of the residents of the State if the interest of one or more of the residents "has been or is threatened or adversely affected." 42 U.S.C. § 1320d-5(d)(1). Statutory damages are provided in the amount calculated by multiplying the number of violations by up to $100, in total not exceeding $25,000 for all violations of an identical provision during a calendar year. 42 U.S.C. § 1320d-5(d)(2).

[2035] 42 U.S.C. § 1320d-5(c). *Cf. generally* Jason W. Davis, *HITECH HIPAA Amendments: New Rules on Breach Notification, Business Associate Compliance, and Enforcement*, HEALTH LAW., June 2009, at 23, 26 (discussing the HITECH Act's new enforcement mechanisms).

[2036] *See* 74 Fed. Reg. 42,740, 42,757 (Aug. 24, 2009).

[2037] HITECH Act § 13402(d)(2), 42 U.S.C. § 17932(d)(2). *Cf.* 45 C.F.R. § 164.414.

This regime is enforced by the FTC which, pursuant to HITECH Act § 13407(g), promulgated the FTC Health Breach Notification Rule[2038] in August 2009.

A PHR vendor is defined as an entity, other than a HIPAA-covered entity, "that offers or maintains a personal health record."[2039] The term "personal health record" is in turn defined as an *electronic* record of individually identifiable health information that is "managed, shared, and controlled *by or primarily for the individual*."[2040] This narrows the scope of PHR vendors in two important ways: (1) vendors of information in paper form are not covered;[2041] and (2) "records managed by or primarily for commercial enterprises, such as life insurance companies that maintain such records for their own business purposes"[2042] are not covered. Examples of PHR vendors include Google Health[2043] and Microsoft HealthVault[2044] which both allow people to gather, organize, and share their health information online.

[2038] FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962 (Aug. 25, 2009) (codified at 16 C.F.R. pt. 318). *Cf.* Michael A. Dowell, *HHS and FTC Release Guidance on HITECH Act Requirements*, J. HEALTH CARE COMPLIANCE, July-Aug. 2009, at 5, 8 et seq. (discussing the proposed rule that was published on Apr. 20, 2009).

[2039] *See* HITECH Act § 13400(18), 42 U.S.C. § 17921(18). An entity is not considered a PHR vendor to the extent that it engages in activities as a business associate of a HIPAA–covered entity. *See* 16 C.F.R. § 318.2(j).

[2040] *See* HITECH Act § 13400(11), 42 U.S.C. § 17921(11); 16 C.F.R. § 318.2(d) and (e) (emphasis added).

[2041] HITECH Act § 13407's reliance on the term "personal health record" (as defined in HITECH Act § 13400(11)) narrows its scope to electronic information. *Cf.* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,967 (Aug. 25, 2009) (stating that "[a]lthough […] breaches of data in paper form can be as harmful as breaches of such data in electronic form, the plain language of the Recovery Act compels the Commission to issue a rule covering only electronic data"). Note that HITECH Act § 13402 relies on the broader term "protected health information" which also includes information in paper form. *See supra.*

[2042] H.R. REP. NO. 111-16, at 490 (2009). *Cf.* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,967 n.61 (Aug. 25, 2009) (reiterating the Congressional findings).

[2043] *See* http://www.google.com/health (last accessed Feb. 10, 2011).

[2044] *See* http://www.healthvault.com (last accessed Feb. 10, 2011).

PHR related entities are defined[2045] as entities other than HIPAA-covered entities (or their business associates) that: (1) offer products or services through the website of a PHR vendor;[2046] (2) offer products or services through the website of a HIPAA-covered entity that offers individuals personal health records;[2047] or (3) access information in a personal health record or send information to a personal health record.[2048]

A third party service provider is defined as an entity that provides services to a PHR vendor "in connection with the offering or maintenance of a personal health record" or to a PHR related entity "in connection with a product or service offered by that entity" and that "holds, uses, or discloses" unsecured "PHR identifiable health information"[2049] as a result of such services.[2050]

[2045] HITECH Act § 13407(a) refers to "each entity described in clause (ii), (iii), or (iv) of section 13424(b)(1)(A)." These are collectively defined as a "PHR related entity" by 16 C.F.R. § 318.2(f).

[2046] *See* HITECH Act § 13424(b)(1)(A)(ii); 16 C.F.R. § 318.2(f)(1).

[2047] *See* HITECH Act § 13424(b)(1)(A)(iii); 16 C.F.R. § 318.2(f)(2). Examples of entities that "offer products or services through the website" of a PHR vendor or a HIPAA-covered entity under 16 C.F.R. § 318.2(f)(1) and (2) include "a web-based application that helps consumers manage medications; a Web site offering an online personalized health checklist; and a brick-and-mortar company advertising dietary supplements online" as well as "search engines […] if they appear on PHR Web sites." However, it is important to note that such entities are only subject to the breach notification requirements if they collect unsecured PHR identifiable information at those websites. *See* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,969 (Aug. 25, 2009).

[2048] *See* HITECH Act § 13424(b)(1)(A)(iv); 16 C.F.R. § 318.2(f)(3). This includes "online applications through which individuals connect their blood pressure cuffs, blood glucose monitors, or other devices so that they can track the results through their PHRs." It also includes "online medication or weight tracking programs that pull information from PHRs." *See* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,969 n.78 (Aug. 25, 2009).

[2049] "PHR identifiable health information" is defined as "individually identifiable health information [as defined in 42 U.S.C. § 1320d(6)] and, with respect to an individual, information: (1) That is provided by or on behalf of the individual; and (2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." *See* 16 C.F.R. § 318.2(d) (rephrasing HITECH Act § 13407(f)(2)).

[2050] 16 C.F.R. § 318.2(h) (rephrasing HITECH Act § 13424(b)(1)(A)(v)). Examples include "entities that provide billing, debt collection, or data storage services to vendors of personal health records or PHR related entities." *See* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,969 (Aug. 25, 2009).

With respect to PHR vendors, HITECH Act § 13407(a) provides that "a breach of security of unsecured PHR identifiable health information that is in a personal health record maintained or offered by [the PHR vendor]" has to be notified to: (1) all citizens and residents of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such a breach of security; (2) the FTC; and (3) if more than 500 residents of a State or jurisdiction were affected, prominent media outlets serving such a State or jurisdiction.[2051] HITECH Act § 13407(a) creates the same obligation for PHR related entities if there is "a breach of security of such information that is obtained through a product or service provided by [the PHR related entity]."[2052]

First, it has to be reiterated that the FTC Health Breach Notification Rule—in contrast to the HHS Breach Notification Rule—only covers individually identifiable health information in *electronic form*. Whether it was "unsecured" depends on whether it was protected through the use of a technology or methodology specified in the guidance[2053] issued by the Secretary of the HHS under HITECH Act § 13402(h)(2).[2054]

Second, it has to be emphasized that the definition of a "breach of security" significantly differs from that provided by the HHS Breach Notification Rule: In accordance with HITECH Act § 13407(f)(1), the FTC Health Breach Notification Rule defines a "breach of security" as

[2051] HITECH Act § 13407(a) does not mention the notification of media outlets. HITECH Act § 13407(c), however, refers to § 13402(e) which also mandates a media notice. Accordingly, the FTC Health Breach Notification Rule, specifically 16 C.F.R. § 318.5(b), requires the notification of prominent media outlets.

[2052] *See* HITECH Act § 13407(a), 42 U.S.C. § 17937(a) (2010). *See also* 16 C.F.R. § 318.3(a).

[2053] *See* Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, 74 Fed. Reg. 42,740, 42,742 (Aug. 24, 2009).

[2054] HITECH Act § 13407(f)(3), 42 U.S.C. § 17937(f)(3); 16 C.F.R. § 318.2(i) (referring to HITECH Act § 13402(h)(2)). *See supra* (discussing the guidance).

the "acquisition of [unsecured PHR identifiable health information of an individual in a personal health record] without the authorization of the individual," whereas "acquisition" is presumed "to include unauthorized access to unsecured PHR identifiable health information unless the [PHR vendor], PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information."[2055] In contrast to the definition provided by HITECH Act § 13400(1)(A) and, more specifically, the HHS Breach Notification Rule, this definition does not include a risk-of-harm requirement. Since the unauthorized acquisition of health information is by itself considered harmful,[2056] no requirement dealing with the risk of (additional) harm is needed.[2057] Regarding the perceived danger of "over-notification,"[2058] the FTC noted that, given the highly personal nature of health information, consumers would want to know if such information was read or shared without authorization.[2059]

[2055] This rebuttable presumption is "intended to address the difficulty of determining whether access to data (i.e., the opportunity to view the data) did or did not lead to acquisition (i.e., the actual viewing or reading of the data)." *See* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,966 (Aug. 25, 2009). Similar to the exceptions provided in the HHS Breach Notification Rule (45 C.F.R. § 164.402), the FTC states that "no breach of security has occurred if an unauthorized employee inadvertently accesses an individual's PHR and logs off without reading, using, or disclosing anything." *See id.*

[2056] The FTC correctly notes that its standard does take harm into account since "notification would not be required in a case where an entity can show that although an unauthorized employee accidentally opened a file, it was not viewed, and therefore there has been no harm to the consumer." *See* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,966 (Aug. 25, 2009).

[2057] *See* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,966 (Aug. 25, 2009) (stating that, "[b]ecause health information is so sensitive," the standard for notification "must give companies the appropriate incentive to implement policies to safeguard such highly sensitive information").

[2058] *See, e.g.,* GOV'T ACCOUNTABILITY OFFICE, PRIVACY: LESSONS LEARNED ABOUT DATA BREACH NOTIFICATION, GAO-07-657, at 2 (2007), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-07-657. (stating that "[s]ending too many notices, based on overly strict criteria, could render all such notices less effective, because consumers could become desensitized to them and fail to act when risks are truly significant").

[2059] FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,967 (Aug. 25, 2009).

Since the definition of the term "breach of security" only mentions the "acquisition" (but not the modification or destruction) of information, the FTC Health Breach Notification Rule—like the HHS Breach Notification Rule—only covers breaches of confidentiality.

Regarding the requirements for timeliness, method, and content of notification as well as the issue of burden of proof, HITECH Act § 13407(c) declares § 13402(c)-(f) applicable. In these areas, the FTC Health Breach Notification Rule therefore only differs slightly from the HHS Breach Notification Rule. Regarding the method of notification, 16 C.F.R. § 318.5(a)(1) provides that a notification via e-mail is sufficient "if the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice." Unlike under the HHS Breach Notification Rule, an agreement with the individual is therefore not required.[2060]

Furthermore, since the Secretary of HHS has no regulatory powers over PHR vendors and PHR related entities, only the FTC—and not the HHS—has to be notified. The notification of the FTC has to be performed by PHR vendors and PHR related entities as soon as possible and in no case later than ten business days following the date of discovery of the breach if 500 or more individuals were affected by the breach.[2061] If fewer than 500 individuals were affected, the entity may maintain a log of all breaches, and submit the log annually to the FTC no later than 60 calendar days following the end of the calendar year.

[2060] *Cf.* 45 C.F.R.. § 164.404(d)(1)(i) (stating that a notification by e-mail is permissible "if the individual agrees to electronic notice and such agreement has not been withdrawn").

[2061] According to the instructions on the FTC's website, a standard form has to be filled out and mailed to the FTC. *See* http://www.ftc.gov/healthbreach/ (last accessed Feb. 10, 2011). These instructions are binding pursuant to 16 C.F.R. § 318.5(c) (stating that notices "shall be provided according to instructions at the Federal Trade Commission's Web site").

It is important to note that the HITECH Act puts the FTC under no obligation to publish a list of PHR vendors and PHR related entities who reported a breach.[2062] Upon receipt of a notification of a breach, the FTC only has to notify the Secretary of HHS of the breach.[2063] However, the Secretary does not have to publish any information about these breaches since they were not suffered by a HIPAA-covered entity.[2064]

As mentioned above, third party service providers are also covered by the FTC Health Breach Notification Rule. They have to notify the PHR vendor or PHR related entity to which they provide their services.[2065] The notification has to be directed to an official designated in a written contract by the PHR vendor or the PHR related entity to receive such notices or, if such a designation is not made, to a senior official at the PHR vendor or PHR related entity.[2066] Furthermore, the third party service provider has to obtain an acknowledgment that the notice was received.[2067] The notification has to include the identification of each customer of the PHR vendor or PHR related entity whose unsecured PHR identifiable health information "has been, or is reasonably believed to have been, accessed, acquired, or

[2062] *But see* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,975 (Aug. 25, 2009) (stating that the FTC intends to make reported information publicly available once consumers have been notified). As of Apr. 21, 2010, the FTC has not published any breach notifications.

[2063] *See* HITECH Act § 13407(d).

[2064] *See* HITECH Act § 13402(e)(4) (stating that Secretary shall make available to the public on the Internet website of the HHS a list that identifies "each covered entity involved in a breach").

[2065] *See* HITECH Act § 13407(b).

[2066] *See* 16 C.F.R. § 318.3(b). *Cf.* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,970 (Aug. 25, 2009) (stating that "the contact points designated by contract should be appropriate decisionmakers with sufficient responsibility and authority to oversee the process of notifying consumers").

[2067] *Cf.* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,970 (Aug. 25, 2009) (stating that "evidence that someone signed for a package or opened an email" is not sufficient since "the communication may not have reached the intended recipient, particularly in a large, busy office").

disclosed" during the breach.[2068] This allows the PHR vendor or PHR related entity to fulfill its notification obligations.

To ensure that a third party service provider (e.g. a cloud computing service provider) is aware that it is dealing with a PHR vendor or PHR related entity, such vendors or entities have to notify a third party service provider of their status as PHR vendors or PHR related entities subject to the FTC Health Breach Notification Rule.[2069]

The FTC's enforcement of the new breach notification obligations for PHR vendors, PHR related entities, and third party service providers commenced on February 22, 2010.[2070] Pursuant to HITECH Act § 13407(e), a violation of the FTC Health Breach Notification Rule is treated as an unfair and deceptive act or practice in violation of a regulation under FTC Act § 18(a)(1)(B)[2071] for which the FTC may issue a cease and desist order[2072] and may bring a civil action for recovery of penalties for knowing violations.[2073]

[2068] *See* 16 C.F.R. § 318.3(b).

[2069] *See id. Cf.* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,970 (Aug. 25, 2009).

[2070] The Rule was effective Sept. 24, 2009, its enforcement, however, was postponed. *See* FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,976 (Aug. 25, 2009) (stating that the FTC "will use its enforcement discretion to refrain from bringing an enforcement action for failure to provide the required notifications for breaches that are discovered before February 22, 2010").

[2071] 15 U.S.C. 57a(a)(1)(B).

[2072] *See* FTC Act § 5(b), 15 U.S.C. § 45(b).

[2073] *See* FTC Act § 5(m), 15 U.S.C. § 45(m).

6.2.5. The Gramm-Leach-Bliley Act

Gramm-Leach-Bliley Act (GLBA)[2074] § 501(b),[2075] mandates that each federal agency with authority over financial institutions[2076] establishes standards "relating to administrative, technical, and physical safeguards" for the protection of the "security and confidentiality" of their customers' nonpublic personal information.[2077]

Subsequently, the FTC, the Securities and Exchange Commission (SEC), the federal banking agencies,[2078] and the National Credit Union Administration (NCUA) have established different security standards.[2079] However, only the federal banking agencies and the NCUA issued additional guidance in 2005, mandating the establishment of an incident response program that also entailed the mandatory notification of security breaches to customers.

[2074] Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338. For a general introduction see Bernard Shull, *Banking, commerce and competition under the Gramm-Leach-Bliley Act*, 47 ANTITRUST BULL. 25 (2002).

[2075] 15 U.S.C. § 6801(b) (2010).

[2076] *See* 15 U.S.C. § 6809(3) (generally defining the term "financial institution" as "any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 [12 U.S.C. § 1843(k)]").

[2077] GLBA § 501(b) further states that the purpose of these standards is: "(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." *Cf. supra* chapter 4.1.2 (discussing GLBA's safeguard requirements).

[2078] The Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS). *Cf.* 12 U.S.C. § 1813(q).

[2079] *See* FTC Safeguards Rule, 67 Fed. Reg. 36,484 (May 23, 2002) (codified at 16 C.F.R. pt. 314); SEC Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333 (June 29, 2000) (codified at 17 C.F.R. pt. 248); Interagency Guidelines Establishing Standards for Safeguarding Customer Information; Final Rule, 66 Fed. Reg. 8,616 (Feb. 1, 2001) (codified at 12 C.F.R. pt. 30, app. B [OCC]; 12 C.F.R. pt. 208, app. D-2, and pt. 225, app. F [Board]; 12 C.F.R. pt. 364, app. B [FDIC]; and 12 C.F.R. pt. 570, app. B [OTS]); NCUA Guidelines for Safeguarding Member Information; Final Rule, 66 Fed. Reg. 8,152 (Jan. 30, 2001) (codified at 12 C.F.R. § 748.0 and pt. 748, app. A). *Cf. supra* chapter 4.1.2.

The Interagency Incident Response Guidance[2080] issued by the federal banking agencies and the identically worded[2081] NCUA Incident Response Guidance[2082] require regulated entities to conduct a reasonable investigation of any incident of "unauthorized access" to "sensitive customer information" to promptly determine "the likelihood that the information has been or will be misused."[2083] If the regulated entity determines that misuse of its information about a customer (i.e. a consumer who is a customer)[2084] "has occurred or is reasonably possible," it should also notify the affected customer as soon as possible.[2085]

"Sensitive customer information" is defined rather narrowly as "a customer's name, address, or telephone number, in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or a personal identification

[2080] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005) (codified at 12 C.F.R. pt. 30, app. B, supp. A [OCC], 12 C.F.R. pt. 208, app. D-2, supp. A and pt. 225, app. F, supp A [Board]; 12 C.F.R. pt. 364, app. B, supp. A [FDIC]; and 12 C.F.R. pt. 570, app. B, supp. A [OTS]). *See id.* at 15,751 (stating that "[t]his Guidance interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and the Interagency Guidelines Establishing Information Security Standards"). *Cf. generally* MARK G. MILONE, INFORMATION SECURITY LAW: CONTROL OF DIGITAL ASSETS § 5.06[3][c] (2009); ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL, STATE AND INTERNATIONAL LAW § 25:8 (2009); Sean C. Honeywill, *Data Security and Data Breach Notification for Financial Institutions*, 10 N.C. BANKING INST. 269, 290 et seq. (2006).

[2081] The NCUA Incident Response Guidance uses the term "member" instead of "customer" but defines it identically. In accordance with its jurisdiction it also uses the term "credit union" instead of "institution" to refer to the entities covered by the regulation.

[2082] Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice; Final Rule, 70 Fed. Reg. 22,764 (May 2, 2005) (codified at 12 C.F.R. § 748.0 and pt. 748, app. B).

[2083] *See* Interagency Incident Response Guidance § III.A; NCUA Incident Response Guidance § III.A.

[2084] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,738 (Mar. 29, 2005) (stating that "customer" means "a consumer who obtains a financial product or service from a financial institution to be used primarily for personal, family, or household purposes, and who has a continuing relationship with the institution" and referring to 12 C.F.R. §§ 40.3(h) [OCC], 216.3(h) [Board], 332.3(h) [FDIC], and 573.3(h) [OTS]). *See* Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice; Final Rule, 70 Fed. Reg. 22,764, 22,766 (May 2, 2005) (stating that "member" means "a consumer who obtains a financial product or service from a credit union to be used primarily for personal, family, or household purposes, and who has a continuing relationship with the credit union").

[2085] *See id.*

number or password that would permit access to the customer's account."[2086] Furthermore it includes "any combination of components of customer information that would allow someone to log onto or access the customer's account."[2087] This definition applies irrespective of whether the information is in paper, electronic, or other form.[2088]

It needs to be emphasized that, irrespective of the likelihood of misuse, the institution's primary federal regulator has to be informed as soon as possible.[2089] A regulated entity might also be required to notify federal law enforcement authorities and to file a Suspicious Activity Report ("SAR").[2090] Furthermore, they are "encouraged" but not "required" to notify the nationwide consumer reporting agencies.[2091]

Regarding the content of the customer notice, the Guidance stipulates that a notice should be given in a clear and conspicuous manner and has to contain the following elements: (1) a description of the incident in general terms; (2) a description of the type of customer information that was the subject of unauthorized access or use; (3) information about what the institution has done to protect the customers' information from further unauthorized access;

[2086] *See* Interagency Incident Response Guidance § III.A.1; NCUA Incident Response Guidance § III.A.1.

[2087] *See id.* For example, a user name and the corresponding password.

[2088] *See* Interagency Incident Response Guidance § I (stating that "customer information" means "any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form, maintained by or on behalf of the institution"); NCUA Incident Response Guidance § I (providing the same definition for "member information").

[2089] *See* Interagency Incident Response Guidance § II.A.1.b; NCUA Incident Response Guidance § II.A.1.b. This allows an institution's regulator "to assess the effectiveness of an institution's response plan, and, where appropriate, to direct that notice be given to customers if the institution has not already done so." *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,741 (Mar. 29, 2005); Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice; Final Rule, 70 Fed. Reg. 22,764, 22,768 (May 2, 2005).

[2090] *See* Interagency Incident Response Guidance § II.A.1.c; NCUA Incident Response Guidance § II.A.1.c (referring to the Agencies' SAR regulations and Agency guidance).

[2091] *See* Interagency Incident Response Guidance § III.B.2; NCUA Incident Response Guidance § III.B.2. The three nationwide consumer reporting agencies are Equifax, TransUnion, and Experian (formerly TRW).

(4) a telephone number that customers can call for further information and assistance; and (5) a reminder that customers need to remain vigilant over the next twelve to twenty-four months, and need to promptly report incidents of suspected "identity theft" to the institution. Additionally, the notice should, if "appropriate," contain a number of items intended to help customers detect and deal with the effects of identity theft.[2092]

The Guidance grants regulated entities a lot of flexibility regarding the method of notice. It only requires that it be delivered in a manner "designed to ensure that a customer can reasonably be expected to receive it."[2093]

Regarding the timeliness of notification, the Guidance provides that customers have to be notified "as soon as possible."[2094] A delay is permissible if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay.[2095]

The Interagency Incident Response Guidance and the NCUA Incident Response Guidance are to be enforced by the respective regulatory agencies by bringing an action against the entity in

[2092] These information items are: (1) recommendation that the customer review account statements and immediately report any suspicious activity; (2) a description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports; (3) a recommendation that the customer periodically obtain credit reports from each nationwide consumer reporting agency; (4) an explanation of how the customer may obtain a credit report free of charge; (5) information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft; and (6) encouragement to report any incidents of identity theft to the FTC using its website or toll-free telephone number. *See* Interagency Incident Response Guidance § III.B.1.a-e; NCUA Incident Response Guidance § III.B.1.a-e.

[2093] *See* Interagency Incident Response Guidance § III.C; NCUA Incident Response Guidance § III.C. An institution "may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically." *See id.*

[2094] *See* Interagency Incident Response Guidance § III.A; NCUA Incident Response Guidance § III.A.

[2095] *See id.*

question.[2096] Courts have consistently held that GLBA § 501(b) does not provide a private right of action.[2097]

6.2.6. The Communications Act

Communications Act[2098] § 222[2099] establishes a duty for telecommunications carriers to protect the confidentiality of customer proprietary network information (CPNI).[2100] Pursuant to this provision, the FCC adopted the CPNI Regulations[2101] which were amended in 2007 to create a duty for carriers to notify "breaches" of customer's CPNI.[2102]

The CPNI Regulations provide that a "breach" occurs "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[2103] This means that, consistent with the scope of § 222 of the Communications Act, only breaches of confidentiality but not breaches of integrity or availability have to be notified.

[2096] *See* 15 U.S.C. § 6805(a).

[2097] *See, e.g., In re* Lentz, 405 B.R. 893, 899 (Bankr. N.D. Ohio 2009) (citing Dunmire v. Morgan Stanley DW Inc., 475 F.3d 956 (8th Cir. 2007); *In re* Southhall, No. 07-00115, 2008 WL 5330001, at *4 (Bankr. N.D. Ala. Dec. 18, 2008); and *In re* French, 401 B.R. 295, 309 (Benkr. E.D. Tenn. 2009)).

[2098] Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934) (codified as amended at 47 U.S.C. § 151 et seq.).

[2099] 47 U.S.C. § 222 (2010). This section was added to the Communications Act by Telecommunications Act of 1996 § 702, Pub. L. No. 104-104, 110 Stat. 56, 148-49 (1996).

[2100] *See* chapter 4.1.5 (discussing the terms "telecommunications carrier" and "CPNI").

[2101] 47 C.F.R. §§ 64.2001-11 (2010). *Cf.* chapter 4.1.5 (describing potential penalties for violations of the CPNI Regulations).

[2102] *See* Customer Proprietary Network Information; Final Rule, 72 Fed. Reg. 31,948 (June 8, 2007). *Cf. generally* ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL, STATE AND INTERNATIONAL LAW § 14:31 (2009).

[2103] 47 C.F.R. § 64.2011(e).

Under the CPNI Regulations, a carrier has to notify the FBI and the United States Secret Service (USSS) of any breach of its customers' CPNI "[a]s soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach."[2104]

A carrier also has to notify its customers of a breach of their CPNI[2105] but may only do so after seven full business days have passed after notification to the USSS and the FBI.[2106] A carrier may only notify its affected customers earlier if it "believes that there is an extraordinarily urgent need to notify [them] sooner" in order to avoid "immediate and irreparable harm" and only after consultation with the relevant investigating agency.[2107] The relevant investigating agency may, on the other hand, direct the carrier not to disclose or notify the breach for an initial period of up to 30 days if it determines that public disclosure or notice to customers would "impede or compromise an ongoing or potential criminal investigation or national security."[2108] This period may be further extended by the agency "as

[2104] 47 C.F.R. § 64.2011(b). A breach report has to be filed electronically at http://www.fcc.gov/eb/cpni (last accessed Feb. 10, 2011; further referring to https://www.cpnireporting.gov). *See id.*

[2105] *See* 47 C.F.R. § 64.2011(c).

[2106] *See* 47 C.F.R. § 64.2011(b)(1). State law that is inconsistent with this requirement is preempted. *See* 47 C.F.R. § 64.2011(f). To justify the fact that significant priority was given to the notification of law enforcement agencies over the notification of customers, the FCC stated that it needed to balance "a customer's need to know with law enforcement's ability to undertake an investigation of suspected criminal activity, which itself might advance the goal of consumer protection." Customer Proprietary Network Information; Final Rule, 72 Fed. Reg. 31,948, 31,950 (June 8, 2007). Dissenting with respect to § 64.2011, FCC Commissioner Michael J. Copps called this approach "needlessly overbroad" because "[i]t fails to distinguish those exigent circumstances in which delayed notification is necessary from what I believe to be the majority of cases in which immediate notification to a victim is appropriate." Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C.R. 6,927, 7,020 (Apr. 2, 2007). *Cf. also* Stephen L. Markus, Note, *Unfair Warning: Breach Notification in The FCC's Enhanced Telephone Records Safeguards,* 18 CORNELL J.L. & PUB. POL'Y 247, 254 (2008) (criticizing the FCC's breach notification rules as not sufficiently taking into account consumer interests).

[2107] *See* 47 C.F.R. § 64.2011(b)(2).

[2108] *See* 47 C.F.R. § 64.2011(b)(3).

reasonably necessary in the judgment of the agency."[2109] The agency's initial direction to the carrier as well as any subsequent extensions have to be provided in writing.[2110]

While the CPNI Regulations establish a detailed recordkeeping requirement,[2111] they do not provide any specific requirements regarding the content of a breach report that is to be submitted to the FBI, the USSS, or to the carrier's customers.[2112] Furthermore, the question of the required method of notification (e.g. by regular mail or by text message) have not been addressed.

6.2.7. The Department of Veterans Affairs Information Security Enhancement Act

The Department of Veterans Affairs Information Security Enhancement Act of 2006,[2113] enacted as Title IX of the Veterans Benefits, Health Care, and Information Technology Act of

[2109] *See id.*

[2110] *See id.*

[2111] *See* 47 C.F.R. § 64.2011(b)(d) (requiring that carriers maintain, for a minimum of 2 years, a (possibly electronic) record of (1) any breaches discovered, (2) notifications made to the USSS, the FBI, and the carriers customers, (3) dates of discovery and notification, (4) a detailed description of the breached CPNI, and (5) the circumstances of the breach).

[2112] Customer Proprietary Network Information; Final Rule, 72 Fed. Reg. 31,948, 31,950 (June 8, 2007) (stating that "[t]he Commission declines to specify the precise content of the notice that must be provided to customers in the event of a security breach of CPNI. [The] Commission recognizes that numerous types of circumstances—including situations other than pretexting—could result in the unauthorized disclosure of a customer's CPNI to a third party. Thus, the Commission leaves carriers the discretion to tailor the language and method of notification to the circumstances.").

[2113] Department of Veterans Affairs Information Security Enhancement Act of 2006, Pub. L. No. 109-461, 120 Stat. 3450 (2006) (codified at 38 U.S.C. §§ 5721-28). This act was primarily a reaction to a widely publicized security breach at the Department of Veterans Affairs. *See* David Stout & Tom Zeller, *Vast Data Cache About Veterans Is Stolen*, N.Y. TIMES, May 23, 2006, *available at* http://www.nytimes.com/2006/05/23/washington/23identity.html; Christopher Lee & Zachary A. Goldfarb, *Stolen VA Laptop and Hard Drive Recovered*, WASH. POST, June 30, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/29/AR2006062900352.html; Chuck Miller, *U.S. Veteran Affairs Department settles data breach case*, SC MAGAZINE, Jan. 28, 2009, *available at* http://www.scmagazineus.com/us-veteran-affairs-department-settles-data-breach-case/article/126518/.

2006,[2114] created a number of obligations for the Secretary of Veterans Affairs (VA) in the event of a "data breach with respect to sensitive personal information that is processed or maintained by the Secretary."[2115] In particular, the Secretary was required to prescribe a regulation addressing the issue of breach notification.[2116]

Pursuant to this obligation, the Interim final rule was issued in 2007[2117] and adopted without change in 2008 as the Final rule[2118] (hereinafter *VA Breach Notification Rule*).

In accordance with 38 U.S.C. § 5727(4), the VA Breach Notification Rule defines the term "data breach" as "the loss or theft of, or other unauthorized access to […] data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data."[2119]

The term "sensitive personal information" is defined comprehensively as "any information about the individual maintained by an agency,"[2120] including (1) education, financial transactions, medical history, and criminal or employment history; and (2) information that can be used to distinguish or trace the individual's identity, including name, Social Security number, date and place of birth, mother's maiden name, or biometric records.[2121]

[2114] Veterans Benefits, Health Care, and Information Technology Act of 2006, Pub. L. No. 109-461, 120 Stat. 3403 (2006).

[2115] *See* 38 U.S.C. § 5724(a) (2010).

[2116] *See* 38 U.S.C. § 5724(b)(1).

[2117] Interim final rule, 72 Fed. Reg. 34,395 (June 22, 2007).

[2118] Final rule, 73 Fed. Reg. 19,747 (Apr. 11, 2008).

[2119] 38 C.F.R. § 75.112.

[2120] 38 C.F.R. § 75.112, 38 U.S.C. § 5727(19).

[2121] *Id.*

It is important to emphasize that the definition of "data breach" does not only cover breaches of "confidentiality"[2122] but also of "integrity."[2123] A loss of "availability,"[2124] however, is not covered.[2125] Furthermore, it also covers information in non-electronic form. The term "unauthorized access" as it is used in the definition of "data breach" includes, but is not limited to "access to an electronic information system"[2126] as well as "viewing, obtaining, or using data containing sensitive personal information in any form or in any VA information system."[2127] However, an "unauthorized access" does not result in a data breach if it is "incidental to the scope of employment."[2128] An unauthorized access also does not constitute a breach if there is no possibility of a "compromise of the confidentiality or integrity of the data."[2129] Lastly it should be noted that the VA Breach Notification Rule also interprets "data

[2122] *See* 38 C.F.R. § 75.112, 38 U.S.C. § 5727(2) (defining "confidentiality" as "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information").

[2123] *See* 38 C.F.R. § 75.112, 38 U.S.C. § 5727(14) (defining "integrity" as "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity").

[2124] *See* 38 U.S.C. § 5727(1) (defining "availability" as "ensuring timely and reliable access to and use of information").

[2125] The Department of Veterans Affairs Information Security Enhancement Act of 2006 clearly recognizes that information security involves confidentiality, integrity, and availability. *See* 38 U.S.C. § 5727(11) (defining "information security" as "protecting information and information systems […] in order to provide integrity, confidentiality, and availability"). The definition of the term "data breach," however, only makes reference to confidentiality and integrity. *See* 38 U.S.C. § 5727(4).

[2126] 38 C.F.R. § 75.113.

[2127] *Id.*

[2128] *See* 38 C.F.R. § 75.112, 38 U.S.C. § 5727(4). *See also* 37 C.F.R. § 75.112 (defining "[u]nauthorized access incidental to the scope of employment" as "access, in accordance with VA data security and confidentiality policies and practices, that is a by-product or result of a permitted use of the data, that is inadvertent and cannot reasonably be prevented, and that is limited in nature"). Examples include "instances when employees of contractors and other entities need access to VA sensitive information in order to perform a contract or agreement with VA but incidentally obtain access to other VA sensitive information." *See* 38 C.F.R. § 75.113.

[2129] 38 C.F.R. § 75.113(b) mentions two examples: (1) encryption; and (2) "the inadvertent disclosure to another entity that is required to provide the same or a similar level of protection for the data under statutory or regulatory authority." It should be noted that (strong) encryption will usually only protect the confidentiality but not the integrity of data. To detect breaches of integrity, electronic signatures could be used.

breach" to include "circumstances in which a user misuses sensitive personal information to which he or she has authorized access."[2130]

The VA Breach Notification Rule only requires the notification of individuals if they are "subject to a reasonable risk for the potential misuse of any sensitive personal information."[2131] The Rule provides two different processes for determining whether such a "reasonable risk" exists: (1) the performance of an independent risk analysis[2132] followed by a determination by the Secretary;[2133] or (2) an "accelerated response" without an independent risk analysis.

In the former case, the independent risk analysis has to be conducted as soon as possible after the data breach. The one conducting the analysis has to be a non-VA entity with relevant expertise in data breach assessment and risk analysis or the VA's Office of Inspector General. The risk analysis has to include a finding concerning whether there is a "reasonable risk that sensitive personal information potentially may be misused."[2134]

[2130] 38 C.F.R. § 75.113. The misuse of personal information is an information privacy issue but not an information security issue. *See supra* chapter 2.2.1 (distinguishing information privacy from information security).

[2131] 38 C.F.R. § 75.117(a).

[2132] *See* 38 C.F.R. § 75.115.

[2133] *See* 38 C.F.R. § 75.116.

[2134] 38 U.S.C. § 5724(a)(1); 38 C.F.R. § 75.115. The analysis further has to address all relevant information, including the following: (a) the nature of the event; (b) assessment of the potential harm to the affected individuals; (c) data breach analysis, as appropriate; and (d) a description of the event, including: (1) the date of occurrence; (2) data elements involved; (3) number of individuals (potentially) affected; (4) individuals or groups (potentially) affected; (5) ease of logical data access to the compromised data in light of the degree of protection for the data, e.g., unencrypted; (6) time the data has been out of VA control; (7) the likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons); and (8) known misuses of data containing sensitive personal information, if any. *See* 38 C.F.R. § 75.115(a)-(d).

Upon receipt of the risk analysis, the Secretary has to make a final[2135] determination as to whether the data breach caused a "reasonable risk for the potential misuse of sensitive personal information."[2136]

An "accelerated response" without an independent risk analysis is only permissible in cases in which there is an "immediate, substantial risk of identity theft"[2137] or in cases where private entities, in the same or a similar situation, would be required to provide notice under Federal law.[2138] An accelerated response effectively requires the Secretary to perform his or her own risk assessment.[2139]

Regarding the method of notice, the VA Breach Notification Rule states that the Secretary has to provide written notification by first-class mail.[2140] If the notice requires urgency because of

[2135] *Cf.* 38 C.F.R. § 75.119 (stating that "[a] determination made by the Secretary under this subpart will be a final agency decision").

[2136] 38 C.F.R. § 75.116(a). In addition to some of the factors that are already included in the risk analysis, the Secretary also has to consider: (1) whether the credit protection services that VA may offer under 38 U.S.C. § 5724 may assist individuals in avoiding or mitigating the results of identity theft; and (2) whether private entities are required under Federal law to offer credit protection services to individuals if the same or similar data of the private entities had been similarly compromised. *See* 38 C.F.R. § 75.116(b). Note that the determination of whether a risk is "reasonable" is necessarily subjective. *Cf. supra* chapter 4.1.10.4 (describing the problems of qualitative risk assessment).

[2137] 38 C.F.R. § 75.114(a)(1).

[2138] 38 C.F.R. § 75.114(a)(2).

[2139] 38 C.F.R. § 75.114(a) states that it is in the Secretary's discretion whether or not to notify individuals. 38 C.F.R. § 75.114(b), however, provides a number of risk-related factors the Secretary's exercise of discretion has to be based on: (1) nature and content of the data; (2) ability of an unauthorized party to misuse the data; (3) ease of logical data access to the data (e.g. whether it was encrypted); (4) ease of physical access to the data; (5) the format of the data (e.g. standard electronic format or paper); (6) evidence indicating that the data may have been the target of unlawful acquisition; (7) evidence that the same or similar data had been acquired from other sources improperly and used for identity theft.

[2140] *See* 38 C.F.R. § 75.117(a).

possible imminent misuse of the information, the Secretary may additionally provide information to individuals "by telephone or other means."[2141]

Where there is insufficient or out-of-date contact information, a substitute notice "such as a conspicuous posting on the home page of VA's Web site and notification in major print and broadcast media" has to be provided.[2142]

The VA Breach Notification Rule also prescribes the minimum content of a notification: (1) a brief description of what happened; (2) a description of the types of personal information involved in the breach; (3) what the agency is doing to investigate the breach, to mitigate losses, and to protect against any further breach; (4) contact procedures, including a toll-free telephone number, an e-mail address, website, and/or postal address;[2143] (5) steps individuals should take to protect themselves from the risk of identity theft; and (6) whether the information was encrypted or protected by other means.[2144]

Regarding the timeliness of a notification, the Rule states that notice has to be provided "promptly" and may only be delayed upon a written lawful request from a Federal agency, in order to "protect data or computer resources from further compromise or to prevent

[2141] 38 C.F.R. § 75.117(c).

[2142] *See* 38 C.F.R. § 75.117(b). The wording "such as" suggests that other forms of substitute notice are also permissible.

[2143] In case of a substitute notice, a toll-free phone number has to be included. *See* 38 C.F.R. § 75.117(b).

[2144] *See* 38 C.F.R. § 75.117(a). Note that these elements are identical to what is required by OMB Memorandum M-07-16 (2007), at 16. *Cf. infra* chapter 6.2.8.

interference with the conduct of an investigation or efforts to recover the data."[2145] However, any delay should not exacerbate the risk or harm to any affected individual.[2146]

Lastly, it should be noted that the Department of Veterans Affairs Information Security Enhancement Act of 2006 also mandates that breaches be notified to specific Committees of the Senate and the House of Representatives.[2147]

6.2.8. OMB Memorandum M-07-16

In May 2007, the Office of Management and Budget (OMB) issued memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."[2148] As part of the work of the Identity Theft Task Force,[2149] this memorandum required federal agencies to develop and implement a breach notification policy by August 22, 2007.

The Memorandum offers a rather vague definition of the term "breach"[2150] and in particular does not address the question whether breaches of data integrity are also covered. However,

[2145] 38 C.F.R. § 75.117(d). Such a request must state an estimated date after which notification will have no adverse effects. *See id.*

[2146] *Id.*

[2147] *See* 38 U.S.C. § 5724(c)(1) (mandating that the Secretary submits promptly to the Committees on Veterans' Affairs of the Senate and House of Representatives a report containing (1) the findings of any independent risk analysis; (2) any determination of the Secretary regarding the existence of a "reasonable risk"; and (3) a description of actions (including notifications) taken after the breach). *See also* 38 U.S.C. § 5724(c)(2) (mandating that the Secretary also submits the report referred to in subsection 1 to the Committees on Armed Services of the Senate and House of Representatives if the breach affected a member of the Army, Navy, Air Force, or Marine Corps or a civilian officer or employee of the Department of Defense).

[2148] Available at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf (last accessed Feb. 10, 2011).

[2149] *See* Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 15, 2006) (establishing the Identity Theft Task Force). *Cf.* THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT—A STRATEGIC PLAN 30 (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf (making a recommendation to "ensure effective, risk-based responses to data breaches suffered by federal agencies").

[2150] *See* OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION 1 n.5

since the Memorandum is focused on risks related to "identity theft,"[2151] it should be construed as only covering breaches of confidentiality. The Memorandum does clarify that "personally identifiable information"[2152] that is in paper form instead of electronic, is also covered.[2153]

A policy for "external breach notification," as it has to be established by every federal agency, has to include the following elements: (1) whether breach notification is required; (2) timeliness of the notification; (3) source of the notification; (4) contents of the notification; (5) means of providing the notification; and (6) public outreach in response to a breach.

To determine whether notification of a breach is required, an agency should perform a risk assessment, considering a wide range of harms (e.g. harm to reputation, harassment, or prejudice).[2154] The Memorandum notes that "notification when there is little or no risk of harm might create unnecessary concern and confusion"[2155] and that "consumers could become numb to [notifications] and fail to act when risks are truly significant."[2156] The following five factors have to be considered to assess the likely risk of harm: (1) the nature of the data

(2007) (stating that "the term 'breach' is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic").

[2151] *See id.* at 1 (stating that the development and implementation of a breach notification policy is required "[a]s part of the work of the Identity Theft Task Force").

[2152] *Id.* at 14 (defining "personally identifiable information" broadly as "information which can be used to distinguish or trace an individual's identity").

[2153] *Id.* at 2 (stating that "[b]reaches subject to notification requirements include both electronic systems as well as paper documents").

[2154] *See id.* at 13.

[2155] *Id.*

[2156] *Id.* at 14 n.40.

elements breached; (2) the number of individuals affected;[2157] (3) the likelihood the information is accessible and usable;[2158] (4) the likelihood the breach may lead to harm;[2159] and (5) the ability of the agency to mitigate the risk of harm.

Regarding the timeliness of a notification, the Memorandum requires that it be performed "without unreasonable delay following the discovery of a breach."[2160] A delay is permissible, however, if consistent with "needs of law enforcement and national security" or "any measures necessary for your agency to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised."[2161]

To demonstrate that the breach has the attention of the chief executive of the organization, notifications should generally be issued by the Agency Head or a designated senior-level individual.[2162]

The mandatory contents of a notification are identical to those under the Department of Veterans Affairs Information Security Enhancement Act of 2006.[2163] Furthermore the notice has to be "concise, conspicuous, [and in] plain language."[2164]

[2157] Confusingly, the Memorandum requires this factor to be considered in a risk assessment to determine *whether* (and not how) a notification should be performed. It states, however, that this factor "should not be the determining factor for whether an agency should provide notification"; it may only "dictate the method(s) you choose for providing notification." *See id.* at 14.

[2158] *See id.* (noting that "[i]f the information is properly protected by encryption, for example, the risk of compromise may be low to non-existent").

[2159] An agency has to consider as harm "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." *Id.* at 13 (citing 5 U.S.C. § 552a(e)(10)). Additionally, it should consider "the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, […] fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem." *See id.*

[2160]*Id.* at 16.

[2161] *Id.*

[2162] *See id.*

When deciding on a method of notification, an agency has to consider: (1) the number of individuals affected; (2) what contact information is available about them; and (3) the urgency with which they need to receive the notice.[2165] Accordingly, telephone notification is considered appropriate in cases of urgency and/or when a limited number of individuals are affected. However, it should be contemporaneous with written notification by first-class mail.

First-class mail notification is the primary means of notification. E-mail notification, on the other hand, is considered problematic, because "individuals change their e-mail addresses and often do not notify third parties of the change."[2166] It may only be appropriate if no known mailing address is available, the individual in question has provided an e-mail address and has expressly given consent to e-mail as the primary means of communication.[2167]

Where an agency does not have sufficient contact information to provide individual notifications, a substitute notice has to be issued. It should consist of a conspicuous posting of the notice on the home page of the agency's website and a notification to major print and broadcast media. Such a notice should include a toll-free phone number where an individual can learn whether or not his or her personal information was affected by the breach.

Lastly, the Memorandum requires federal agencies to consider a public outreach in response to a breach. Beyond the notifications discussed above, this entails careful planning, posting

[2163] *Id.* at 16-17. *Cf. supra* chapter 6.2.7 (discussing the content requirements under the Department of Veterans Affairs Information Security Enhancement Act of 2006).

[2164] OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION 16 (2007).

[2165] *See id.* at 17.

[2166] *Id.* at 18.

[2167] *See id.*

breach-related information on the home page of the agency's website, notification of other public and private sector agencies, and being prepared to respond to inquires from other governmental agencies such as the Government Accountability Office and Congress.[2168]

6.2.9. The EU ePrivacy Directive

The only legal act under EU law that implements a data security breach notification regime is Parliament and Council Directive 2002/58[2169] (hereinafter *ePrivacy Directive*). The notification regime was introduced into the ePrivacy Directive by Parliament and Council Directive 2009/136[2170] (hereinafter *Citizens' Rights Directive* or *CRD*) which was adopted as part of the "Telecoms Package."[2171]

The new data security breach notification regime has to be transposed by Member States by May 25, 2011.[2172] Article 4(3) of the ePrivacy Directive as amended by the CRD constitutes the core of the breach notification regime. The first two sentences of this provision state:

> In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.
>
> When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

[2168] *See id.* at 19.

[2169] 2002 O.J. (L 201) 37 (EC).

[2170] 2009 O.J. (L 337) 11 (EC).

[2171] This legislative package consists of three legal acts: the Citizens' Rights Directive, Parliament and Council Directive 2009/140, 2009 O.J. (L 337) 37 (EC), and Parliament and Council Regulation 1211/2009, 2009 O.J. (L 337) 1 (EC).

[2172] *See* CRD art. 4.

The personal scope of application of the ePrivacy Directive's breach notification regime is therefore limited to "provider[s] of publicly available electronic communications services" which covers in particular Internet access providers but not online service providers.[2173]

The notification obligation is triggered by a "personal data breach" which is defined in ePrivacy Directive article 2(h):

> a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.

Thus, ePrivacy Directive article 4(3) does not only cover breaches of confidentiality ("unauthorised disclosure" or "[unauthorised] access") but also breaches of integrity ("alteration") as well as permanent losses of availability ("unlawful destruction" or "loss").[2174] This is remarkable insofar, as most other data security breach notification regimes discussed *supra* only apply to breaches of confidentiality.

As regards the type of information covered, the ePrivacy Directive uses the term "personal data" which is broadly defined by the EUDPD as "information relating to an identified or identifiable natural person"[2175] whether or not in electronic form.[2176]

Under the ePrivacy Directive's breach notification regime, the obligation to notify government authorities is rather broad: Pursuant to the first sentence of ePrivacy Directive

[2173] *See supra* chapter 4.1.9 (discussing the legal definition of the term "publicly available electronic communications service").

[2174] *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 44 (2010) (F.R.G.).

[2175] EUDPD art. 2(a). *Cf.* ePrivacy Directive art. 2 (stating that "[s]ave as otherwise provided, the definitions in Directive 95/46/EC […] shall apply").

[2176] EUDPD art. 2(b) (defining "processing of personal data" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means […]").

article 4(3), a provider of a publicly available electronic communications service has to notify the "competent national authority" of *all* personal data breaches without "undue delay." In this context, it has to be pointed out that the ePrivacy Directive does not obligate the competent national authorities to make the received notifications available to the provider's subscribers or the general public.[2177]

The second sentence of ePrivacy Directive article 4(3) mandates that communications service providers notify any personal data breach to "the subscriber or individual […] without undue delay." However, this only applies if the breach in question "is likely to adversely affect the personal data or privacy of a subscriber or individual."[2178]

The ePrivacy Directive does not define what constitutes an adverse effect on "personal data or privacy." Recital 61 of the CRD at least provides a non-exhaustive list of adverse effects: "for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community."[2179] This clarifies that, by itself, a personal data breach does not sufficiently adversely affect the personal data or privacy of a subscriber or an individual. Thus, the "likely" occurrence of further damages—beyond the breach itself—is required for a "personal data breach" to trigger a communications service provider's obligation to notify subscribers and individuals concerned.[2180]

[2177] *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 45 (2010) (F.R.G.).

[2178] ePrivacy Directive art. 4(3).

[2179] CRD recital 61.

[2180] *See* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 45 (2010) (F.R.G.).

The ePrivacy Directive thereby significantly reduces the number of cases in which subscribers and individuals are to be notified because breaches of the security of most kinds of personal data are not likely at all to cause significant further damages (e.g. a breach concerning one's name, address, marital status, telephone number, e-mail address, relatives' names, or profession).[2181]

Recital 61 of the CRD lays out the rationale for limiting the obligation to notify subscribers and individuals to cases where consequential damages are likely to occur: Subscribers and individuals "should be notified without delay in order to allow them to take the necessary precautions."[2182]

Whether a particular personal data breach is likely to have adverse effects as described above is initially to be determined by the communications service provider itself. However, the ePrivacy Directive implements an important control mechanism[2183]: the competent national authorities which have to be notified of all personal data breaches—that is, irrespective of whether the breach is likely to have adverse effects—may order the communications service provider to notify the subscribers and individuals after "having considered the likely adverse effects of the breach."[2184]

The ePrivacy Directive further frees communications service providers from any obligations to notify the subscribers and individuals if they can demonstrate "to the satisfaction of the

[2181] *See* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 45 (2010) (F.R.G.).

[2182] CRD recital 61.

[2183] *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 45 (2010) (F.R.G.).

[2184] ePrivacy Directive art. 4(3).

competent authority that [they have] implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach."[2185]

As regards the mandatory content of the notifications that are to be provided to subscribers or individuals, the ePrivacy Directive requires communications service provides to at least (a) describe the nature of the data breach, (b) inform about the contact points where more information can be obtained, and (c) recommend measures to mitigate the possible adverse effects of the personal data breach.[2186]

The wording of ePrivacy Directive article 4(3) remarkably does not require communications service providers to inform subscribers and individuals about which of their personal data has been affected by the security breach.[2187] The provision's wording also does not require that providers disclose how many subscribers and individuals were affected.[2188]

Additional information items have to be included in the notifications to be sent to the competent national authorities: (a) a description of the "consequences of […] the personal

[2185] ePrivacy Directive art. 4(3). This includes in particular strong encryption processes.

[2186] ePrivacy Directive art. 4(3).

[2187] *Cf.* Lukas Feiler, *Security Breach Notification: Informationspflichten bei der Verletzung der Sicherheit personenbezogener Daten* [*Security Breach Notification: Obligations to Notify Breaches of the Security of Personal Data*], in PRAXISSCHRIFT FÜR WOLFGANG ZANKL – INNOVATION UND INTERNATIONALE RECHTSPRAXIS [INNOVATION AND INTERNATIONAL LEGAL PRACTICE: FESTSCHRIFT FOR WOLFGANG ZANKL] 147, 161 (Lukas Feiler & Maximilian Raschhofer eds., 2009) (arguing that the stated purpose of the Directive's notification regime—to allow subscribers and individuals to take precautionary measures—may at least in some situations require providers to disclose which types of personal information have been affected by a breach).

[2188] If not legally required, providers are unlikely to disclose this information because they "want to make sure that the content of the notifications does not impact negatively on customer relations." *See* ENISA, DATA BREACH NOTIFICATIONS IN THE EU 5 (2011), *available at* http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport.

data breach"[2189] and (b) a description of the "measures proposed or taken by the provider to address the […] breach."[2190] Furthermore, it can be argued that notifications to competent national authorities should contain a third and a fourth additional information item[2191]:

First, recital 58 of the CRD provides that the competent national authorities "should have […] *comprehensive* and reliable data about security incidents that have led to the personal data of individuals being compromised."[2192] Incident data could, however, hardly be considered "comprehensive" if it does not include information about the number of individuals affected.[2193]

Second, as discussed *supra*, ePrivacy Directive article 4(3) grants the competent national authorities the power to order a communications service provider to notify subscribers and individuals concerned after "having considered the likely adverse effects of the breach."[2194] Potential adverse effects cannot, however, be assessed without having been informed about the type of personal data affected.[2195]

[2189] ePrivacy Directive art. 4(3).

[2190] *Id.*

[2191] *See* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 45 (2010) (F.R.G.).

[2192] CRD recital 58 (emphasis added).

[2193] *See* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 45 (2010) (F.R.G.).

[2194] ePrivacy Directive art. 4(3).

[2195] *See* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 45 (2010) (F.R.G.).

Accordingly, ePrivacy Directive article 4(3) should be construed as mandating that the competent national authorities be also notified about (1) the number of individuals concerned and (2) the types of personal data affected.[2196]

As regards the "circumstances, format and procedures" of breach notifications, article 4(5) of the ePrivacy Directive empowers the Commission to "adopt technical implementing measures."[2197]

A more specific guidance regarding in particular the "circumstances" under which subscribers and individuals are to be notified is in fact much needed because the notification trigger provided by the ePrivacy Directive leaves a lot of room for interpretation.[2198] What degree probability is needed for adverse effects to be considered "likely" and what—in addition to the examples given in CRD recital 61—constitutes an adverse effect in the first place?

Guidance is also needed regarding the "format" of breach notifications.[2199] Is it sufficient for communications service providers to notify their subscribers and the individuals concerned by an electronic message such as an e-mail or a text message? Or do they have to send the notifications by regular mail, which would be considerably more expensive? Furthermore, do

[2196] *See id. Cf. also* ENISA, DATA BREACH NOTIFICATIONS IN THE EU 18-19 (2011), *available at* http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport (noting that national regulatory authorities have indicated that notifications should include (1) a description of the nature of the breach; (2) information about the nature of the data exposed; (3) the number of people affected; and (4) information about what is being done to contain the breach).

[2197] The last sentence of ePrivacy Directive art. 4(5), read in conjunction with ePrivacy Directive art. 14a(2) provides that the adoption has to be performed under the "regulatory procedure with scrutiny" pursuant to Council Decision 1999/468, art. 5a(1) to (4) and art. 7, 1999 O.J. (L 184) 23 (EC), as amended.

[2198] *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 46 (2010) (F.R.G.).

[2199] *Cf. id.*

communications service providers have to pay for the publication of the breach notice in a newspaper if they have no contact details for some of the individuals concerned?

The Commission would be well-advised to adopt technical implementing measures that answer the questions raised above. Without such clarifications, a great deal of legal uncertainty would continue to exist, allowing Member States to implement national notification regimes that might differ significantly from one another, in particular regarding the ultimate costs of individual notifications. Counter to the ePrivacy Directive's purpose of harmonizing national law to "avoid obstacles to the internal market for electronic communication,"[2200] such divergent national notification requirements would distort competition between communications service providers operating in different Member States.[2201]

To enforce the ePrivacy Directive's notification regime, the competent national authorities have to be able to "audit whether providers have complied with their notification obligations."[2202] To facilitate such audits, communications service providers have to maintain an "inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken."[2203]

[2200] ePrivacy Directive recital 8.

[2201] *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 46 (2010) (F.R.G.); Karin Retzer, *Data Breach Notification: The Changing Landscape in the EU*, 2 COMPUTER L. REV. INT'L 39, 42 (2008) (F.R.G.) (emphasizing the importance of uniformity of national data security breach notification requirements).

[2202] ePrivacy Directive art. 4(4).

[2203] ePrivacy Directive art. 4(4). Thus, this inventory has to contain more information than has to be included in a notification to the competent national authority. *Cf.* ePrivacy Directive art. 4(4) (stating that the inventory has to "be sufficient to enable the competent national authorities to verify compliance with [art. 4(3)]"). *Cf. also* CRD recital 58 (stating that communications service providers should "maintain an inventory of personal data breaches to enable further analysis and evaluation by the competent national authorities").

If a communications service provider fails to perform the required breach notifications, the competent national authorities have to be empowered to "impose appropriate sanctions,"[2204] including penalties that must be effective, proportionate and dissuasive.[2205] Such penalties may be applied to cover the period of any breach, even where the breach has subsequently been "rectified."[2206]

6.2.10. Comparative Assessment

As a preliminary matter, it has to be noted that there is significantly more legislative activity in this area in the U.S. than in the EU: There are six different data security breach notification regimes currently implemented in U.S. federal law. Additionally, 46 of the 50 states (including California and New York), the District of Columbia, Puerto Rico, and the Virgin Islands have implemented data security breach notification laws.[2207] Some states, such as California, have even implemented multiple breach notification regimes.[2208]

[2204] ePrivacyDirective art. 4(4). *Cf.* Parliament and Council Directive 2009/140, recital 51, 2009 O.J. (L 337) 37 (EC) (stating that the experience in the implementation of the EU regulatory framework indicates that existing provisions empowering national regulatory authorities to impose fines have failed to provide an adequate incentive to comply with regulatory requirements). *Cf. also Commission Staff Working Document, Impact Assessment,* at 107, SEC (2007) 1472 (Nov. 13, 2007) (stating that "[a] survey of the situation in various Member States demonstrated that light sanctions and uneven enforcement have in some cases led to ineffective or insufficient protection of consumer rights in the areas covered by the ePrivacy Directive").

[2205] *See* ePrivacy Directive art. 15a(1).

[2206] *Id*.

[2207] *See* http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (last accessed Feb. 11, 2011).

[2208] *See supra* chapters 6.2.1 (discussing California Senate Bill 1386) and 6.2.2 (discussing California Senate Bill 541).

In comparison, EU law only provides a single (sector-specific) regulation. Out of the 27 EU Member States, only two, Austria[2209] and Germany,[2210] have adopted legislation that requires the notification of data security breaches.[2211]

6.2.10.1. Policy Objectives

The objectives pursued by the different data security breach notification regimes discussed above can be generally classified as either addressing the threat of impersonation fraud[2212] or generally strengthening information privacy.

New York ISBNA and the regulations issued under GLBA § 501(b), by only covering information that can be used to commit "identity theft,"[2213] solely attempt to address the risk of impersonation fraud.[2214]

[2209] *See* Datenschutzgesetz 2000 [DSG] [Data Protection Act 2000], BGBl. I No. 165/1999, as amended by DSG-Novelle 2010 [DSG Amendment 2010], BGBl. I No. 133/2009, § 24(2a). *Cf.* Lukas Feiler, *Data Breach Notification nach österreichischem Recht* [*Data Breach Notification under Austrian Law*], 5 MEDIEN UND RECHT 281 (2009) (Austria).

[2210] *See* Bundesdatenschutzgesetz [Federal Data Protection Act], Jan. 14, 2003, BGBl. I at 66, as amended by Gesetz zur Änderung datenschutzrechtlicher Vorschriften [Act to Amend Data Protection Provisions], Aug. 14, 2009, BGBl. I at 2814, § 42a (F.R.G.).

[2211] Until Germany enacted its data security breach notification provision in August 2009, not a single Member State had adopted a breach notification regime. *See* STEWART DRESNER & AMY NORCUP, PRIVACY LAWS & BUSINESS, DATA BREACH NOTIFICATION LAWS IN EUROPE 12 (2009), *available at* http://www.privacylaws.com/templates/EventPage.aspx?id=1410. Ireland's data protection authority has adopted a "Personal Data Security Breach Code of Practice," which is, however, not legally binding. *See* http://www.dataprotection.ie/docs/07/07/10_-_Data_Security_Breach_Code_of_Practice/1082.htm (last accessed Feb. 10, 2011). *Cf.* ENISA, DATA BREACH NOTIFICATIONS IN THE EU 12 (2011), *available at* http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport (briefly comparing the legal situation in Germany, Spain, the U.K., and Ireland).

[2212] *Cf. supra* chapter 4.1.10.1 (discussing the nature of impersonation fraud).

[2213] *See* N.Y. STATE TECH. LAW § 208(1)(a), N.Y. GEN. BUS. LAW § 899-aa(1)(b) (defining "private information" as "personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account"); Interagency Incident Response Guidance § III.A.1 and NCUA Incident Response Guidance § III.A.1 (defining Sensitive customer information" is defined rather narrowly as "a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, On the other hand, the following breach notification regimes cover all personal information and are therefore best characterized as information privacy measures: the VA Breach Notification Rule,[2215] OMB Memorandum M-07-16,[2216] and the ePrivacy Directive.[2217] The following are also information privacy measures but have a narrower (sector specific) scope: California Senate Bill 541 (covering medical information),[2218] the HHS Breach Notification Rule (covering protected health information),[2219] the FTC Health Breach Notification Rule (covering PHR identifiable health information),[2220] and the regulations issued under Communications Act § 222 (covering CPNI).[2221]

credit or debit card number, or a personal identification number or password that would permit access to the customer's account).

[2214] *Cf.* Brendan St. Amant, *The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 HARV. J. ON LEGIS. 505, 523 (2007) (arguing that the risk of identity theft is a poor trigger because "database breaches can have serious repercussions that have nothing to do with stealing identities or the associated economic loss").

[2215] *See* 38 C.F.R. § 75.112 (defining "sensitive personal information" as "any information about the individual maintained by an agency").

[2216] *See* OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION 14 (2007) (defining "personally identifiable information" as "information which can be used to distinguish or trace an individual's identity").

[2217] *See* ePrivacy Directive art. 2(h) (referring to "personal data" which is defined as "information relating to an identified or identifiable natural person").

[2218] *See* CAL. HEALTH & SAFETY CODE § 1280.15(a)(1) (referring to CAL. CIV. CODE § 56.05(g) which defines "medical information" as "individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment")

[2219] *See* HITECH Act § 13400(12), 42 U.S.C. § 17921(12) (referring to 45 C.F.R. § 160.103 which defines "protected health information" as "individually identifiable health information […] transmitted or maintained in any […] form or medium").

[2220] "PHR identifiable health information" is defined as "individually identifiable health information [as defined in 42 U.S.C. § 1320d(6)] and, with respect to an individual, information: (1) That is provided by or on behalf of the individual; and (2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." *See* 16 C.F.R. § 318.2(d) (rephrasing HITECH Act § 13407(f)(2)).

[2221] See 47 C.F.R. § 64.2003(g) which refers to 47 U.S.C. § 222(h)(1) (defining customer proprietary network information (CPNI) as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a

California Senate Bill 1386 covers a middle ground since it, when it was adopted, only covered information that could be used to commit impersonation fraud[2222] but was amended in 2007 by California Assembly Bill 1298[2223] and now also covers medical information[2224] and health insurance information.[2225]

The policy objective of seven of the ten data security breach notification regimes therefore is to strengthen information privacy, while only three specifically address the risk of impersonation fraud.

telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information").

[2222] *See* CAL. CIV. CODE §§ 1798.29(e), 1798.82(e) (amended 2007) (defining "personal information" as "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.").

[2223] 2007 Cal. Legis. Serv. Ch. 699 (West).

[2224] *See* CAL. CIV. CODE §§ 1798.29(f)(2), 1798.82(f)(2) (defining "medical information" as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional").

[2225] *See* CAL. CIV. CODE §§ 1798.29(f)(3), 1798.82(f)(3) (defining "health insurance information" as "an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records"). According to the legislative history, these two provisions are "aimed at the problem of medical identity theft and, more generally, a patient's right to keep medical information private." *Personal Information: Disclosure: Hearing on A.B. 1298 Before the Assem. Comm. on Judiciary* 5 (Cal. 2007), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_cfa_20070409_110459_asm_comm.html. Medical identity theft occurs "when someone uses an individual's name and sometimes other identifying information without the individual's knowledge to obtain medical services or products." *See* CAL. DEP'T OF CONSUMER AFF., OFF. OF PRIVACY PROT., RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 5 (2009), *available at* http://www.privacy.ca.gov/res/docs/pdf/COPP_Breach_Reco_Practices_6-09.pdf.

6.2.10.2. Risk Treatment Options

Generally speaking, a breach notification regime can be used to implement two different risk treatment options: *indirect risk mitigation*[2226] and *indirect risk transfer*.[2227] Both options are of an indirect nature because the effects of breach notifications will only develop if regulated entities comply with the notification regime.[2228]

If implemented as a risk mitigation measure, a breach notification regime may focus on enabling reactive measures[2229] by affected individuals and/or enabling deterrent measures[2230] by law enforcement agencies.

The only breach notification regime that just requires the notification of affected individuals but not of any public authority, thereby aiming to mitigate risk exclusively by enabling individuals to take reactive measures is California Senate Bill 1386.[2231] Taking an almost contrary approach, the CPNI Regulations under Communications Act § 222 grant the notification of law enforcement agencies a much higher priority than the notification of individuals.[2232] All other breach notification regimes put a strong emphasis on the notification of the affected individuals but nevertheless either additionally require the notification of a law enforcement agency,[2233] at least mandate the notification of a regulatory authority (which may

[2226] *See supra* chapter 3.2.1.2.

[2227] *See supra* chapter 3.2.3.2.

[2228] *See supra* chapters 3.2.1.2 and 3.2.3.2 (describing the difference between direct and indirect risk treatment).

[2229] *See supra* chapter 3.1 (introducing the concept of reactive security measures).

[2230] *See id.* (introducing the concept of deterrent security measures).

[2231] *See supra* chapter 6.2.1.

[2232] *See supra* chapter 6.2.6.

[2233] This is the case for New York ISBNA (requiring, *inter alia*, the notification of the state attorney general if New York residents are affected; *see supra* chapter 6.2.3).

in turn notify a law enforcement agency),[2234] or, in the first place, only apply to public authorities (which may inform a law enforcement agency themselves).[2235]

There is, however, a significant problem when data security breach notification regimes are implemented in attempt to mitigate risks: They rarely work.

The requirement of the notification of individuals for the purpose of enabling them to take reactive measures is based on the assumption that there are measures individuals can take to reduce their risk. This is, however, rarely the case. When the confidentiality of sensitive personal information (e.g. medical information or call records) has been compromised, there is indeed very little an affected individual can to do to reduce potential harms to his reputation or reduce the extent to which his privacy will be violated due to the effects of the security breach. There are only two plausible cases in which individuals can reasonably take reactive security measures: First, if the confidentiality of passwords has been compromised, users can react by changing their passwords.[2236] Second, when identifying information that can be used to commit impersonation fraud has been compromised, consumers could, albeit burdensome, contact the three national consumer reporting agencies to request a "security freeze"[2237] or

[2234] This is the case for California Senate Bill 541 (requiring notification of the California Department of Public Health; *see supra* chapter 6.2.2), the HHS Breach Notification Rule (requiring notification of the Secretary of HHS; *see supra* chapter 6.2.4.1), the FTC Health Breach Notification Rule (requiring notification of the FTC), the regulations issued under GLBA § 501(b) (requiring notification of the institution's primary federal regulator; *see supra* chapter 6.2.5), and the ePrivacy Directive (requiring notification of a competent national authority; *see supra* chapter 6.2.9).

[2235] This is the case for OMB Memorandum M-07-16 (*see supra* chapter 6.2.8) and the VA Breach Notification Rule (*see supra* chapter 6.2.7).

[2236] Passwords are typically stored in an encrypted fashion. However, even moderate computer resources are often sufficient to "crack" many passwords within a reasonable timeframe. For a list of tools that are used in practice see MICHAEL CROSS, SCENE OF THE CYBERCRIME 481 et seq. (2d ed. 2008).

[2237] *See supra* chapter 4.1.7.4.

regularly monitor their credit reports.[2238] However, as discussed *supra* in chapter 4.1.10.1, any attempt to fight impersonation fraud by focusing on the "theft" of identifying information—rather than the problem of authentication of consumers before extending credit to them—is fundamentally flawed. Furthermore, evidence that would support the assumption that a breach of identifying information actually increases the risk of impersonation fraud is very limited.[2239]

Any attempt to mitigate risk by enabling law enforcement agencies to implement deterrent measures in the form of criminal prosecution also faces a fundamental challenge. In most cases, the perpetrator simply cannot be identified.[2240]

In summary, data security breach notification is rather poorly suited to (indirectly) mitigate information security risks. However, risk mitigation is not the only risk treatment option available.[2241]

[2238] *Cf.* FTC, FTC Consumer Alert: What To Do If Your Personal Information Has Been Compromised (Mar. 2005), http://ftc.gov/bcp/edu/pubs/consumer/alerts/alt150.shtm.

[2239] *See* GOV'T ACCOUNTABILITY OFFICE, DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN, GAO-07-737 (2007), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-07-737 (finding that most breaches have not resulted in detected incidents of identity theft); SASHA ROMANOSKY ET AL., DO DATA BREACH DISCLOSURE LAWS REDUCE IDENTITY THEFT? 13-14 (SEVENTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, WORKING PAPER, 2008), *available at* http://weis2008.econinfosec.org/papers/Romanosky.pdf (finding that data breach notification laws had no statistically significant effect on reducing identity theft). *Cf.* KRISTIN M. FINKLEA, CONG. RESEARCH SERV., IDENTITY THEFT: TRENDS AND ISSUES, CRS REPORT FOR CONGRESS R40599, at 20 (2010), *available at* http://opencrs.com/document/R40599/2010-01-05/download/1013/; Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1125-26 (2009).

[2240] *See infra* chapter 7.4.1 (discussing the attribution problem on the Internet).

[2241] *Cf.* Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1126 (2009) (also recognizing this possibility and referring to it as the "[improvement of] organizational data security practices"—as opposed to "identity theft"); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 306 (2005) (citing Ethan Preston & Paul Turner, *The Global Rise of A Duty to Disclose Information Security Breaches*, 22 J. MARSHALL J. COMPUTER & INFO. L. 457, 460 (2004) (stating that "[r]equiring businesses to disclose information security violations [also] provides operators with a market incentive to ensure that their security is adequate")). *Cf. also* Jacques S. Gansler & William Lucyshyn, *Improving the Security of Financial Management Systems: What are We to Do?*, A data security breach notification regime can also be used to implement an indirect risk transfer. However, many of the regimes discussed above ignore potential positive effects other than risk mitigation[2242]: They either do so explicitly[2243] or by establishing a risk-of-harm requirement for the notification of individuals.[2244] Indeed, the only breach notification regime that explicitly hints at another possibility than risk mitigation is the FTC Health Breach Notification Rule which states that a notification regime also "give[s] companies the appropriate incentive to implement policies to safeguard such highly sensitive information."[2245]

Organizations that store, process, or transmit personal information are typically best positioned to mitigate risks to that information. However, they currently only bear a small portion of these risks, leading to a misalignment between risk and risk mitigation capability.[2246] To a significant extent, this misalignment is caused by the fact that individuals

24 J. ACCT. & PUB. POL'Y 1, 7 (2005) (stating that in the absence of incentives for information sharing created by the private sector, "the federal government should develop incentives to encourage full and open sharing of computer security vulnerability and incident data").

[2242] Alternative benefits are also often ignored in the literature. *See, e.g.,* MICHAEL TURNER, TOWARDS A RATIONAL PERSONAL DATA BREACH NOTIFICATION REGIME 19 (2006), *available at* http://perc.net/files/downloads/data_breach.pdf (only considering how notified consumers might react quickly to prevent "identity theft").

[2243] *See* HHS Breach Notification Rule, 74 Fed. Reg. 42,740, 42,765 (Aug. 24, 2009) (stating that the only other benefit—besides allowing individuals to take reactive measures to prevent identity theft—was "enabling an affected individual to mitigate harm to his or her personal reputation that may result from the exposure of sensitive medical information").

[2244] This is the case for the regulations issued under GLBA § 501(b) (requiring information misuse "has occurred or is reasonably possible"; *see supra* chapter 6.2.5), the VA Breach Notification Rule (requiring a "reasonable risk for the potential misuse"; *see supra* chapter 6.2.7), OMB Memorandum M-07-16 (noting that "notification when there is little or no risk of harm might create unnecessary concern and confusion"; *see supra* chapter 6.2.8), and the ePrivacy Directive (requiring that the breach is "likely adversely affecting" personal data or privacy by causing harm such as "identity theft or fraud, physical harm, significant humiliation or damage to reputation"; *see supra* chapter 6.2.9).

[2245] FTC Health Breach Notification Rule; Final Rule, 74 Fed. Reg. 42,962, 42,966 (Aug. 25, 2009).

[2246] *See supra* chapter 2.4.4 (discussing the misalignment between risk and risk mitigation capability as one of the fundamental challenges of information security).

(and other third parties) do not have sufficient information to assess the level of security provided by a particular organization.[2247] Without such information they cannot take security into account when deciding whether to change to a competitor or, in the case where the individual concerned is not a customer of the organization, request that his personal information be deleted (if such a right is granted under applicable law).[2248] As discussed in chapter 3.2.3.2, targeted transparency policies can be used to address this deficiency.[2249]

The effects of data security breach notification as a targeted transparency policy depend on whether the the information contained in breach notifications (hereinafter referred to as *breach information*) becomes "embedded" into the decision-making processes of current and potential customers (referred to in this context as *information users* or *users*).[2250] To achieve embeddedness, three requirements have to be fulfilled:

First, users have to perceive the breach information to have value for achieving higher levels of security for their personal information.[2251] Breach information is only likely to have such value if it allows a comparison of different competitors. However, how should such a comparison be performed if breach notifications are not publicly available from a central repository? Indeed, the HHS Breach Notification Rule is the only regime under which breach

[2247] *See* chapter 2.4.3 (discussing the uninformed risk decisions and the difficulty of measuring security as one of the fundamental challenges of information security).

[2248] *Cf.* EUDPD art. 12(b).

[2249] *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 39 (2007) (discussing how targeted transparency policies differ from warnings (i.e. risk mitigation)).

[2250] *See supra* chapter 3.2.3.2 (discussing in general terms how targeted transparency policies can lead to an indirect risk transfer). *Cf.* Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1128 (2009) (discussing data security breach notification with regard to "targeted transparency").

[2251] *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 55 (2007).

notices are to be collected centrally and, at least partly, made publicly available.[2252] None of the other breach notification regimes provides such a central public repository of breach information, thereby making it very difficult to perform any comparisons.[2253]

Second, the available breach information has to be compatible with users' decision-making processes in particular with regard to the breach information's format and time and place of availability.[2254] Ideally, breach information should be available when and where users make their buying decisions (e.g. on the log-in screen in the case of an online service). However, depending on the users' habits for making choices with regard to certain goods or services, it may also be sufficient if the breach information is available in consumer-specific publications or, in particular with regard to online services, on well-known central websites. Again, the only breach notification regime that remotely fulfills this requirement is the HHS Breach Notification Rule.[2255]

Third, breach information has to be easily comprehensible for users.[2256] It is this requirement where all breach notification regimes fail most spectacularly. Data security breach notification policies are often rightly criticized for leaving users confused about (1) what actually has happened and (2) what they should personally do about it.[2257] To some extent, this problem is

[2252] *See supra* chapter 6.2.4.1.

[2253] For example, the website DataLossDB.org currently attempts to "accumulate more [breach] notices via the Freedom of Information Act, and its various local and state legislative cousins." *See* http://datalossdb.org/primary_sources (last accessed Feb. 10, 2011). Note that a central repository is also essential to achieve compatibility with users' decision-making processes (*see infra*).

[2254] *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 56 (2007).

[2255] *See supra* chapter 6.2.4.1.

[2256] *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 59 (2007).

[2257] *See* PONEMON INST., NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION 3 (2005), *available at* http://www.whitecase.com/files/FileControl/863d572d-cde3-4e33-903c-37eaba537060/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/Security_Breach_Survey%5B1%5D.pdf (stating that "48% of respondents caused by a lack of relevant information: all breach notification regimes either do not require any specific information to be included in the breach notices[2258] or do not require the inclusion of highly relevant information such as the number of individuals affected.[2259] However, even if all relevant information was included in a breach notice, users would likely be overwhelmed by the information presented to them. To address this problem, a government agency could act as an intermediary, translating each centrally published breach report into a single metric that indicates the severity of the breach on an easily comprehensible scale.[2260]

Given that the three requirements are fulfilled by neither of the data security breach notification regimes, these regimes are unlikely to have long-lasting effects on the users' buying decisions once users have become accustomed to regularly reading about data security breaches.[2261]

said that the notice was not easy to understand, and over 49% of respondents believed that the notice did not provide enough details"). *Cf. also* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches,* 105 MICH. L. REV. 913, 951 (2007).

[2258] This is the case for California Senate Bill 1386 (*see supra* chapter 6.2.1), California Senate Bill 541 (*see supra* chapter 6.2.2), and the CPNI Regulations issued pursuant to Communications Act § 222 (*see supra* chapter 6.2.6). *Cf.* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches,* 105 MICH. L. REV. 913, 947 (2007) (noting that notification letters currently only supply "non-comparative information about data security").

[2259] This is the case for all breach notification regimes except California Senate Bills 1386, 541, and the CPNI Regulations which do not require *any* specific information to be included (see previous note).

[2260] *See infra* chapter 9.1.2 (proposing a data security breach notification regime based on targeted transparency).

[2261] *Cf.* ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 71 (2008) (noting that as people come to expect that breaches occur, they will be less likely to withdraw their business because of them).

6.2.10.3. What Constitutes a Breach

Despite a lot of discussion in the EU and the U.S. about the notification of "data breaches," the definitions provided by the various notification regimes differ significantly regarding the question of how to define a breach.

The first important issue is whether the definition of a breach should cover confidentiality, integrity, and also availability. The notification regimes that are focused on impersonation fraud are naturally only concerned with confidentiality.[2262] Many of the privacy-focused notification regimes that were adopted in the U.S. are unfortunately still based on the "secrecy paradigm"[2263] and therefore also only consider information confidentiality.[2264] Others additionally cover unauthorized use of information[2265] which is an information privacy but not an information security concern.[2266] In the U.S., the only exception is the VA Breach Notification Rule which also covers breaches of the integrity of information.[2267]

[2262] These are the New York ISBNA and the regulations issued under GLBA § 501(b). *See supra* chapter 6.2.10.1.

[2263] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 42 (2004) (noting that privacy problems have been understood as invasions into one's hidden world and emphasizing that this conception of privacy is inadequate to address many problems of electronic databases); *cf. also* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 119 (2010) (referring to it as the "public/private dichotomy").

[2264] This is the case for California Senate Bill 1386 (*see supra* chapter 6.2.1), the regulations issued under GLBA § 501(b) (*see supra* chapter 6.2.5), and OMB Memorandum M-07-16 (*see supra* chapter 6.2.8).

[2265] This is the case for California Senate Bill 541 (*see supra* chapter 6.2.2), HHS Breach Notification Rule (*see supra* chapter 6.2.4.1), and the CPNI Regulations issued under Communications Act § 222 (*see supra* chapter 6.2.6).

[2266] *See supra* chapter 2.2.1 (distinguishing information privacy from information security).

[2267] *See supra* chapter 6.2.7.

Since EU data protection policy is not based on the secrecy paradigm,[2268] the ePrivacy Directive covers losses of confidentiality and integrity as well as permanent losses of availability.[2269]

Individuals do not only have an interest in the confidentiality but also in the integrity and availability of their information. This is particularly the case with regard to health information, the integrity and availability of which may be critical in medical emergencies. Similarly, the integrity of financial information or call records can be highly important since both types of information are often used in criminal prosecutions. In this regard, the VA Breach Notification Rule and, even more so, the ePrivacy Directive have clear advantages over the other breach notification regimes.

The second issue of importance is under which circumstances a covered entity has to assume that a breach has occurred. Pursuant to California Senate Bill 1386 and New York ISBNA, an "unauthorized acquisition" is required.[2270] The FTC Health Breach Notification Rule also requires an "acquisition" but provides the rebuttable presumption that any "unauthorized access" enabled an "acquisition."[2271]

In contrast to the rather high standard of "acquisition," all other breach notification regimes only require "unauthorized access."[2272] Even going one step further, the following regimes also cover an unauthorized "disclosure" (which may or may not lead to unauthorized

[2268] *Cf. supra* chapter 2.2.1.

[2269] *See supra* chapter 6.2.9 (discussing that the ePrivacy Directive covers "destruction, loss, alteration, unauthorised disclosure of, or access to personal data").

[2270] *See supra* chapters 6.2.1 and 6.2.3.

[2271] *See* 16 C.F.R. § 318.2(a).

[2272] *See supra* chapters 6.2.2, 6.2.4.1, 6.2.5, 6.2.6, 6.2.7, 6.2.8, and 6.2.9.

access)[2273]: California Senate Bill 541, the HHS Breach Notification Rule, the CPNI Regulations issued under Communications Act § 222, OMB Memorandum M-07-16, and the ePrivacy Directive.[2274]

In this context, it should be pointed out that—unlike in the physical world where theft is easily detectable by looking for tangible objects that have been taken—the acquisition of information is very difficult to detect. For example, operating systems often keep no records of the fact that a certain file has been copied to a remote server.[2275] Even if they do, such records can typically be falsified once the malicious threat agent has gained administrative privileges on an operating system. However, what is much easier to detect than the acquisition of information is when a computer system is being compromised, thereby permitting unauthorized access to personal information.

A notification regime that uses "unauthorized access" rather than "acquisition" as a notification trigger therefore makes it much more certain for regulated entities to discover breaches. Particularly if a notification regime also aims to perform a risk transfer by creating targeted transparency,[2276] it should not ignore breaches that "only" consist in unauthorized

[2273] For example, if an internal customer database was inadvertently made available via the business's public website, customer information would be "disclosed" irrespective of whether anyone accessed the database.

[2274] *See supra* chapters 6.2.2, 6.2.4.1, 6.2.6, 6.2.8, and 6.2.9.

[2275] UNIX and Linux operating systems typically only store the time of last access (the "atime") for each file but do not record the identity of the user who accessed the file. *See* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 130 (3d ed. 2003). While additionally logging capabilities have been available for a long time, they are rarely used in practice. *See* SCOTT MANN & ELLEN L. MITCHELL, LINUX SYSTEM SECURITY: THE ADMINISTRATOR'S GUIDE TO OPEN SOURCE SECURITY TOOLS 171 (2d ed. 2000) (describing the Linux utility "auditd"); CHARLIE RUSSEL ET AL., MICROSOFT WINDOWS 2000 SERVER ADMINISTRATOR'S COMPANION 713 (2d ed. 2003) (describing Windows 2000's capability to log any file access). Depending on the server software used to transfer the file, that server software may create log entries for file transfers (e.g. FTP servers and HTTP servers typically create such log entries). However, once a malicious threat agent has gained access to a system account, he may easily circumvent these application-based logging mechanisms.

[2276] *See supra* chapter 6.2.10.2.

access to information since such breaches are equally valuable for judging an organization's level of security. For the same reasons, the "unauthorized disclosure" of personal information should be used as an additional notification trigger.

The third issue, which is related to the second, is that of encryption. Under California Senate Bill 1386 and New York ISBNA, it does not constitute a breach if the information in question was "encrypted." This is a rather unfortunate wording since encryption does not equate to security: The level of protection provided by encryption depends on the strength of the design and implementation of the encryption algorithm as well as the confidentiality and complexity of the decryption key.[2277] New York ISBNA only considers the latter aspect by narrowing the exemption for encrypted information to instances where the encryption key[2278] has not been compromised.

The HHS Breach Notification Rule and the FTC Breach Notification rule take a more reasonable approach to encryption and refer to a guidance issued by the Secretary of HHS which takes both aspects into account by (1) referring to standards issued by the National Institute of Standards and Technology (NIST) with regard to encryption processes and (2) emphasizing the importance of the confidentiality of the decryption key.[2279] OMB

[2277] *Cf.* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 102 et seq. (2000); Steve Stanek, *Auditing Cryptography: Assessing System Security, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1023, 1024 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (stating that "[s]ecurity professionals who use cryptography rely on two factors for the security of the information protected by the cryptographic systems: (1) the rigor of the algorithm against attack and (2) the secrecy of the key that is used to encrypt the sensitive information.").

[2278] As previously noted, New York ISBNA is ignorant of the fact that the encryption key is only the same as the decryption key if a symmetric cryptographic algorithm is used. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 4 (2d ed. 1996).

[2279] *See* Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, 74 Fed. Reg. 42,740, 42,742 (Aug. 24, 2009).

Memorandum M-07-16 and the VA Breach Notification Rule also exempt properly encrypted information but do not provide any guidance for determining the required encryption strength.[2280]

6.2.10.4. Notification of Individuals Concerned

Due to their focus on risk mitigation rather than targeted transparency, the following breach notification regimes only require the notification of the individuals concerned if there is a risk of harm: the HHS Breach Notification Rule,[2281] the regulations issued under GLBA § 501(b),[2282] the VA Breach Notification Rule,[2283] OMB Memorandum M-07-16,[2284] and the ePrivacy Directive.[2285]

The FTC Health Breach Notification Rule, in accordance with its dual focus on risk mitigation and transparency,[2286] explicitly notes that "consumers would want to know if [health] information was read or shared without authorization."[2287]

[2280] *See* OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION 12 n.34 (2007) (allowing the exemption of "properly encrypted" information); 38 C.F.R. § 75.113(b) (exempting information that has been encrypted in a way that there is "no possibility of compromising the confidentiality or integrity of the data").

[2281] Indeed, the HHS Breach Notification Rule includes a risk-of-harm requirement in its definition of the term "breach." *See supra* chapter 6.2.4.1.

[2282] The notification of individuals is only required if misuse "has occurred or is reasonably possible" (*see supra* chapter 6.2.5).

[2283] Notification is only required if there is a "reasonable risk" of misuse. *See supra* chapter 6.2.5.

[2284] *See supra* chapter 6.2.8.

[2285] *See supra* chapter 6.2.9.

[2286] *See supra* chapter 6.2.10.2.

[2287] FTC Health Breach Notification Rule; Final Rule; 74 Fed. Reg. 42,962, 42,967 (Aug. 25, 2009). This statement is more akin to a right to know policy than a targeted transparency policy. *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 28 (2007) (describing the difference between a right to know and targeted transparency).

The method of notification to individuals is an issue that is addressed in great detail by all notification regimes except by the CPNI Regulations[2288] and the ePrivacy Directive which leaves this issue to technical implementing measures that are still to be adopted by the European Commission.[2289] To the extent that notifications have to be sent by traditional mail[2290] they can be rather costly. Given that the risk mitigation effect of breach notifications is rather limited,[2291] such costly notification requirements effectively amount to a penalty which is rightly being criticized as inappropriate in many cases because data breaches often occur despite the entity having practiced due care.[2292]

6.2.10.5. Enforcement

Almost all of the discussed breach notification regimes exclusively provide public enforcement mechanisms. The only exceptions are California Senate Bill 1386 which additionally implements a private enforcement mechanism by allowing "customers" to

[2288] *See supra* chapter 6.2.6.

[2289] *See supra* chapter 6.2.9.

[2290] California Senate Bill 541 and VA Breach Notification Rule only permit notifications via regular mail. California Senate Bill 1386, New York ISBNA, the regulations issued under GLBA § 501(b), the HHS Breach Notification Rule, and OMB Memorandum M-07-16 primarily require a notification by regular mail but permit a notification via e-mail if prior consent has been given. The FTC Health Breach Notification Rule also primarily requires a notification by regular mail but provides an opt-out rather than an opt-in mechanism for notifications via e-mail.

[2291] *See supra* chapter 6.2.10.2.

[2292] *Cf.* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 193 (2007) (stating that data breach notification laws would amount to a punishment of software buyers for the iniquities of software manufacturers which are responsible for the majority of vulnerabilities that are exploited to breach data security). *Cf. also* Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1133, 1159 (2009) (stating that data security breach notification laws "establish an inequitable strict liability regime because when breaches occur they do not distinguish between companies that implement information security best practices and those that show a reckless disregard for the security of sensitive data").

institute a civil action to recover damages and seek an injunction[2293] and the VA Breach Notification Rule which does not provide any enforcement mechanism at all.[2294]

All mandatory disclosure policies and in particular targeted transparency policies[2295] heavily depend on strong and effective enforcement mechanisms. To reduce the risk that regulated entities may capture the regulatory system,[2296] multiple public authorities could be tasked with its enforcement. In this regard, the HHS Breach Notification Rule serves as an excellent example. It is to be enforced not only by the Secretary of the HHS who has to impose civil penalties in cases of willful neglect but also by the State attorneys general who may bring *parens patriae* actions to seek injunctions and damages on behalf of the residents of their state.[2297]

6.2.10.6. Conclusion

An analysis of the data security breach notification regimes currently implemented in U.S. federal law, California and New York state law, and EU law reveal significant differences, in particular with regard to the policy objective ("identity theft" v. general protection of information privacy), the definition of what actually constitutes a "breach," and under which conditions to notify the individuals concerned.

[2293] *See supra* chapter 6.2.1.

[2294] *See supra* chapter 6.2.7.

[2295] *See* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 45 (2007).

[2296] In particular in situations where the costs of regulatory compliance are concentrated on few regulated entities while the benefits of compliance are dispersed, the regulated entities are well positioned to capture the regulatory process. *See* James Q. Wilson, *The Politics of Regulation, in* THE POLITICS OF REGULATION 370 (James Q. Wilson ed., 1980) (noting that "[s]ince the incentive to organize is strong for opponents of the policy but weak for the beneficiaries, and since the political system provides many points at which opposition can be registered, it may seem astonishing that regulation of this sort is ever passed"). *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 110 (2007) (noting that concentrated costs and dispersed benefits are typical for targeted transparency policies).

[2297] *See supra* chapter 6.2.4.1.

However, with the exception of the VA Breach Notification Rule and the ePrivacy Directive, they all focus on the confidentiality and ignore the integrity and availability of information. With the exception of the FTC Breach Notification Rule they are all also exclusively concerned with risk mitigation by allowing affected individuals and/or law enforcement agencies to take reactive security measures. They do so despite the fact that there is little evidence to support the assumption that individuals are at all capable to mitigate their risks after having been notified of a breach.

The possibility of performing an indirect risk transfer by providing targeted transparency has not received sufficient consideration in any of the analyzed breach notification regimes.

6.3. Mandatory Network Security Breach Notification

The term network security breach notification, as used in this thesis, generally describes a policy that requires communications network providers to notify all breaches of network security to a public authority and/or to subscribers. This policy is distinct from data security breach notification[2298] insofar as it focuses on the availability of communications networks and services as opposed to the security of personal information. Network security breach notification is an issue that is closely related to the policy area of Critical Information Infrastructure Protection (CIIP).[2299]

In the U.S., network security breach notification regimes are currently implemented in federal regulations as well as in California law. The latter, however, will not be addressed specifically

[2298] *See supra.*

[2299] *Cf. supra* chapter 2.2.2.

in this chapter because it dynamically refers to federal regulations "as modified by [the Federal Communications Commission] over time."[2300]

6.3.1. The FCC Network Outage Reporting Rule

The FCC Network Outage Reporting Rule[2301] which became effective on January 3, 2005[2302] requires certain types of communications providers to report information about significant outages to the Federal Communications Commission (FCC).

6.3.1.1. Personal Scope of Application

The personal scope of application of the FCC Network Outage Reporting Rule covers (1) cable communications providers that provide circuit-switched telephony,[2303] (2) operators of Interexchange Carrier (IXC) tandem facilities and Local Exchange Carrier (LEC) tandem facilities,[2304] (3) satellite communications providers,[2305] (4) satellite operators,[2306] (5)

[2300] Decision Adopting General Order 133-C and Addressing Other Telecommunications Service Quality Reporting Requirements, D.09-07-019, 2009 Cal. PUC LEXIS 320 (Cal. P.U.C., July 16, 2009). General Order 133-C § 4(a) states that the California Public Utilities Commission (CPUC) adopts, "for its major service interruption reporting," the FCC Network Outage Reporting Rule "as modified by FCC over time."

[2301] Disruptions to Communications; Final Rule, 69 Fed. Reg. 70,316 (Dec. 3, 2004) (codified at 47 C.F.R. pt. 4 and § 63.100).

[2302] *See* Announcement of effective date, 69 Fed. Reg. 78,338 (Dec. 30, 2004).

[2303] *See* 47 C.F.R. § 4.3(a) (defining "[c]able communications providers" as "cable service providers that also provide circuit-switched telephony").

[2304] *See* 47 C.F.R. § 4.3(a) (defining "IXC or LEC tandem facilities" as "tandem switches (or their equivalents) and interoffice facilities used in the provision of interexchange or local exchange communications"). Interexchange Carriers (IXCs) primarily carry long-distance calls between Local Exchange Carriers (LECs). *Cf.* CHARLES H. KENNEDY, AN INTRODUCTION TO U.S. TELECOMMUNICATIONS LAW 1, 103 (2d ed. 2001) (describing the regulatory origin of these terms).

[2305] *See* 47 C.F.R. § 4.3(d) (describing "[s]atellite communications providers" as providers that "use space stations as a means of providing the public with communications, such as telephony and paging").

[2306] *See id.* (defining "[s]atellite operators" as "entities that operate space stations but do not necessarily provide communications services directly to end users").

Signaling System 7 (SS7)[2307] providers, (6) wireless service providers,[2308] (7) wireline communications providers,[2309] and (8) affiliated and non-affiliated entities that maintain or provide communications networks or services used by any of the aforementioned providers in offering their communications (third party providers).[2310] However, these providers are only covered to the extent that they provide "for a fee to one or more unaffiliated entities" one of the following services: (1) "two-way voice [communications]," (2) "data communications, paging service," or (3) "SS7 communications."[2311] The second type of services raises the question whether Internet access providers or Internet backbone providers[2312] are also covered. In this regard, the FCC's Notice of Proposed Rule Making (NPRM)[2313] clarifies that the FCC did not intend "at this time, to adopt reporting requirements for public data networks"[2314] which are defined broadly as "[any] network that provides data

[2307] SS7 is the control protocol used to provide instructions to the various elements within a circuit-switched telephony network or, as 47 C.F.R. §4.3(e) puts it, "is a signaling system used to control telecommunications networks." *See* TRAVIS RUSSELL, SIGNALING SYSTEM #7, at 1 (5th ed. 2006). *See also* ITU, INTRODUCTION TO CCITT SIGNALLING SYSTEM NO. 7, ITU-T RECOMMENDATION Q.700 (1993), *available at* http://www.itu.int/rec/T-REC-Q.700-199303-I/en.

[2308] *See* 47 C.F.R. § 4.3(f) (stating that "[w]ireless service providers" include "Commercial Mobile Radio Service [CMRS] communications providers that use cellular architecture and CMRS paging providers").

[2309] 47 C.F.R. § 4.3(g) defines "[w]ireline communications providers" as providers which "offer terrestrial communications through direct connectivity, predominantly by wire, coaxial cable, or optical fiber, between the serving central office (as defined in the appendix to part 36 of this chapter) and end user location(s)." The term "central office" is defined in the glossary that is provided by 47 C.F.R. pt. 36, app. as "[a] switching unit, in a telephone system which provides service to the general public […]."

[2310] *See* 47 C.F.R. § 4.3(a), (d), (e), (f), and (g). Explicitly excluded are equipment manufacturers and vendors if they "do not maintain or provide communications networks or services used by communications providers in offering communications." *See* 47 C.F.R. § 4.3(h).

[2311] 47 C.F.R. § 4.3(b) (defining the term "communications provider").

[2312] *Cf. supra* chapter 2.3.1 (describing Internet access providers and Internet backbone providers from a technical perspective).

[2313] FCC Notice of Proposed Rule Making, FCC 04-30, ET Docket No. 04-35, at 4 n.4 (Feb. 23, 2004).

[2314] *Id* at 4 n.4.

communications for a fee to one or more unaffiliated entities."[2315] Furthermore, the FCC Network Outage Reporting Rule also states that it will only cover communications providers "that provide voice and/or paging communications."[2316] This effectively reduces the FCC Network Outage Reporting Rule's personal scope of application to providers of "switched voice and paging communications."[2317] However, as discussed *infra*, some outage reports are nevertheless relevant for the availability of services offered over the Internet.[2318]

6.3.1.2. Expanding the Personal Scope to Broadband Providers?

It should be noted that the FCC's National Broadband Plan recommended that the FCC "should expand its outage reporting requirements to broadband service providers."[2319] Whether the FCC actually has jurisdiction over broadband service providers has been called into question by a ruling issued by the D.C. Circuit Court of Appeals less than a month after the National Broadband Plan had been published.[2320] The court held that the FCC could not

[2315] *Id. See also* FCC Report and Order and Further Notice of Proposed Rule Making, FCC 04-188, ET Docket No. 04-35, Aug. 19, 2004, at 4 n.2 (reiterating that public data networks should not be covered).

[2316] Disruptions to Communications; Final Rule, 69 Fed. Reg. 70,316, 70,316 (Dec. 3, 2004). *See also* 47 C.F.R. § 4.9(c)(5) (referring to service which "are never used to carry common carrier voice or paging communications" as "non-covered services").

[2317] On its website, the FCC states that, "in sum," the reporting requirements only apply to providers of "switched voice and paging communications." *See* http://www.fcc.gov/pshs/techtopics/techtopics15.html (last accessed Feb. 10, 2010). Voice over Internet Protocol (VoIP) telephony is also not covered. *See* FCC Report and Order and Further Notice of Proposed Rule Making, FCC 04-188, ET Docket No. 04-35, Aug. 19, 2004, at 61. *See also* FCC, FCC PREPAREDNESS FOR MAJOR PUBLIC EMERGENCIES 26 (2009), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-293332A1.pdf (stating that "[t]oday, the FCC does not require ISPs to file outage information akin to that received from traditional communications providers under the Part 4 rules").

[2318] *See infra* chapter 6.3.1.3.

[2319] FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 321 (2010), *available at* http://www.broadband.gov/download-plan/. The National Broadband Plan was adopted pursuant to American Recovery and Reinvestment Act of 2009, § 6001(k), Pub. L. No. 111-5, 123 Stat. 115, 516 (2009).

[2320] Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010) (holding that FCC lacked ancillary authority to regulate Internet service provider's network management practices).

rely on its "ancillary jurisdiction"[2321] under Title I of the Communications Act[2322] without tying it to a "statutorily mandated responsibility."[2323] Since the FCC had not relied on a suitable statutorily mandated responsibility in its order against Comcast,[2324] the court vacated it. In reaction to this decision, the FCC announced its intention to reclassify broadband services—which are currently classified as "information services" under Title I of the Communications Act—as "telecommunications services" under Title II over which the FCC does not only have "ancillary jurisdiction" but also direct authority.[2325] This reclassification is, however, likely to be challenged in court since the Supreme Court, in deference to the FCC's technical expertise,[2326] upheld the FCC's 2002 ruling to classify broadband services as "information services."[2327]

[2321] Communications Act of 1934 § 4(i), 47 U.S.C. § 154(i) ("The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions.").

[2322] Communications Act of 1934, Pub. L. No. 416, 48 Stat. 1064 (1934) (codified at 47 U.S.C. § 151 et seq. as amended).

[2323] *See* Am. Library Ass'n v. FCC, 406 F.3d 689, 700 (D.C. Cir. 2005) (holding that the FCC's ancillary jurisdiction is limited to circumstances where: (1) the FCC's general jurisdictional grant under Title I of the Communications Act of 1934 covers the subject of the regulations and (2) the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities).

[2324] *See* Free Press v. Comcast Corp., 23 F.C.C.R. 13028 (2008). Comcast had blocked the network traffic of peer-to-peer (P2P) applications which raised the issue of "net neutrality". *See id* at 13053.

[2325] *See* JULIUS GENACHOWSKI, CHAIRMAN OF THE FCC, THE THIRD WAY: A NARROWLY TAILORED BROADBAND FRAMEWORK (2010), *available at* http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0506/DOC-297944A1.pdf.

[2326] Under the *Chevron* doctrine which was also applied by the Court in this case, courts may not substitute their own construction of a statutory provision for a reasonable interpretation made by an agency if the legislative delegation to the agency on a particular question is implicit rather than explicit. Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837, 844 (1984).

[2327] Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967 (2005) (upholding the FCC's ruling that cable companies providing broadband Internet access did not provide a "telecommunications service" under Title II but an "information service" under Title I). *See* AUSTIN SCHLICK, GENERAL COUNSEL AT THE FCC, A THIRD-WAY LEGAL FRAMEWORK FOR ADDRESSING THE COMCAST DILEMMA 7 (2010), *available at* http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0506/DOC-297945A1.pdf (suggesting that the FCC should in particular rely on Justice Scalia's dissent in *Brand X* which was joined by Justices Souter and Ginsburg).

6.3.1.3. Outages Subject to Mandatory Reporting

Covered providers are only required to report "outages"[2328] that last at least 30 minutes and (1) meet certain user-based thresholds, (2) meet certain capacity-based thresholds, (3) potentially affect specific aspects of 911 communications,[2329] (4) potentially affect special offices and facilities (e.g., major military installations),[2330] or (5) result in a failure of certain critical elements of the network.[2331]

User-based thresholds are either expressed in "user minutes" or in "blocked calls." The former is a metric that is defined as the mathematical result of multiplying the duration of an outage, expressed in minutes, by the number of end users potentially affected by the

[2328] *See* 47 C.F.R. § 4.5(a) (defining "outage" as "a significant degradation in the ability of an end user to establish and maintain a channel of communications as a result of failure or degradation in the performance of a communications provider's network").

[2329] *See* 47 C.F.R. § 4.5(e). 911 is the emergency telephone number used in the U.S. Potential effects on 911 communications are relevant for cable communications providers, satellite communications providers, wireless service providers, wireline communications providers, and their respective third party providers. *See* 47 C.F.R. § 4.9(a)(4), (c)(2)(iv), (e)(5), and (f)(4).

[2330] *See* 47 C.F.R. § 4.5(d) (defining "[s]pecial offices and facilities" as "major military installations, key government facilities, nuclear power plants, and those airports that are listed as current primary (PR), commercial service (CM), and reliever (RL) airports in the FAA's National Plan of Integrated Airports Systems (NPIAS)"). The member agencies of the National Communications System (NCS) will determine which of their locations are "major military installations" and "key government facilities." *See id.* For a list of the NCS member agencies see http://www.ncs.gov/mem_orgs.html (last accessed Feb. 10, 2011). The effects on special offices and facilities are relevant for cable communications providers, satellite communications providers, wireless service providers, wireline communications providers, and their respective third party providers. *See* 47 C.F.R. § 4.9(a)(3), (c)(2)(iii), (e)(4), and (f)(3).

[2331] For satellite operators, these critical elements are: satellite transponders, satellite beams, inter-satellite links, entire satellites, and, in the case of Mobile-Satellite Service ("MSS") satellite operators, gateway earth stations. *See* 45 C.F.R. § 4.9(c)(1). For satellite communications providers these elements are satellites or transponders. *See* 45 C.F.R. § 4.9(c)(2)(i). For wireless service providers, there is only one critical element, a Mobile Switching Center (MSC). *See* 45 C.F.R. § 4.9(e)(1).

outage.[2332] User-based thresholds are established for all providers except satellite operators.[2333]

Capacity-based thresholds are expressed in "DS3 minutes" which are defined as the mathematical result of multiplying the duration of an outage (in minutes), by the number of previously operating DS3 circuits that were affected by the outage.[2334] The FCC correctly notes that "there may, on occasion, be [DS3] service disruption reporting by cable, wireline, and wireless service providers that includes transmission paths that support public data networks."[2335] This means that despite only covering providers of switched voice and paging communications, the FCC will nevertheless also receive some reports about outages affecting the Internet. The FCC Network Outage Reporting Rule provides a threshold of 1,350 DS3 minutes[2336] for cable communications providers, wireless service providers, wireline communications providers, IXC and LEC tandem facilities, and their respective third party providers.[2337]

[2332] *See* 47 C.F.R. § 4.7(e)(2). For telephony and for those paging networks in which each individual user is assigned a telephone number, the sum of working telephone numbers potentially affected by the outage is used instead of the number of potentially affected users. *See* 47 C.F.R. § 4.7(e)(1).

[2333] For cable communications providers, satellite communications providers, wireless service providers, wireline communications providers, and their respective third party providers, the threshold is 900,000 user minutes. *See* 47 C.F.R. § 4.9(a)(1), (c)(2)(ii), (e)(2), and (f)(2). For IXC and LEC tandem facilities, and SS7 providers, the threshold is 90,000 blocked calls or, if history data is used to determine the effects of the outage, 30,000 blocked calls. *See* 47 C.F.R. § 4.9(b) and (d).

[2334] A DS3 circuit (sometimes also referred to as a T3 circuit) can handle 28 DS1s (T1s), 672 DS0 (64 kilobit per second voice or data circuits), or a total bandwidth of 44.736 megabit per second. *Cf.* Disruptions to Communications; Proposed rule, 69 Fed. Reg. 15,761, 15,766 (Mar. 26, 2004).

[2335] FCC Report and Order and Further Notice of Proposed Rule Making, FCC 04-188, ET Docket No. 04-35, Aug. 19, 2004, at 62 n.341.

[2336] This equals a bandwidth of about 60 gigabit per second.

[2337] *See* 47 C.F.R. § 4.9(a)(2), (b), (e)(3), and (f)(2).

6.3.1.4. When and How to Report Outages

When discovering an outage that meets one of the conditions described above, a covered communications provider has to submit electronically[2338]: (1) a basic notification within 120 minutes,[2339] (2) an Initial Communications Outage Report within 72 hours,[2340] and (3) a Final Communications Outage Report within 30 days.[2341]

Each of these three submissions has to contain the following information: the name of the reporting entity; the date and time of onset of the outage; a brief description of the problem; the particular services affected; the geographic area affected by the outage; and a contact name and contact number by which the FTC's technical staff may contact the reporting entity.[2342]

The notification may be limited to the most basic information[2343] while the Initial Communications Outage Report should be more detailed, covering "all pertinent information then available"[2344] and the Final Communications Outage Report "shall contain all pertinent

[2338] *See* 47 C.F.R. § 4.11 (stating that "[s]ubmitted electronically" refers to "submission of the information using Commission-approved Web-based outage report templates").

[2339] *See* 47 C.F.R. § 4.9(a), (c)(1), (c)(2), (d), (e), and (f).

[2340] *See* 47 C.F.R. § 4.9(a)(4), (c)(3), (d), (e)(5), and (f)(4).

[2341] *See id.*

[2342] *See* 47 C.F.R. § 4.11 (listing the mandatory information items of Initial and Final Communications Outage Reports). *See* Disruptions to Communications; Final Rule, 69 Fed. Reg. 70,316, 70,330 (Dec. 3, 2004) (listing the same mandatory information items for notifications).

[2343] *See* Disruptions to Communications; Final Rule, 69 Fed. Reg. 70,316, 70,330 (Dec. 3, 2004) (stating that the "bare-bones notification" will not substantially divert communications providers from their repair and restoration efforts immediately after onset of the outage but will alert the FTC to the possibility that a major communications outage might be occurring).

[2344] 47 C.F.R. § 4.11.

information on the outage, including any information that was not contained in, or that has changed from that provided in, the Initial report."[2345]

6.3.1.5. Public Access to Outage Reporting Information

The issue of whether the FCC should publicly disclose the outage information reported to it has been hotly debated. Under the old FCC rule that was introduced in 1992 and only covered wireline communications providers,[2346] all information reported pursuant to the rule was made publicly available by the FCC. In 1992, the FCC reasoned that "[t]he public is entitled to full and forthcoming explanations of [telephone service outages]."[2347] The FCC further stated that one purpose of requiring notification was "to serve as a source of information for the public, to encourage and, where appropriate, to assist in dissemination of information to those affected."[2348]

Contrary to the FCC's previous reasoning, the FCC Network Outage Reporting Rule as it is currently in force, presumes all outage reports "to be confidential"[2349] and withholds the reports from disclosure to the public in accordance with the Freedom of Information Act[2350] (FOIA). Citing concerns raised by the Department of Homeland Security, the FCC reasoned that "[t]he disclosure of outage reporting information to the public could present an unacceptable risk of more effective terrorist activity," in particular with regard to "those [communications] networks, which are part of our Nation's critical information

[2345] *Id.*

[2346] 57 Fed. Reg. 7,883 (Mar. 5, 1992) (codified at 47 C.F.R. § 63.100).

[2347] 57 Fed. Reg. 7,883, 7,884 (Mar. 5, 1992).

[2348] *Id.*

[2349] 47 C.F.R. § 4.2.

[2350] Freedom of Information Act, Pub. L. No. 89-554, 80 Stat. 383 (1996), as amended.

infrastructure."[2351] This reversal was particularly relevant for providers other than wireline communications providers which were not covered under the old rule. All information they voluntarily reported to the FCC was not subject to disclosure under the FOIA because the Critical Infrastructure Information Act of 2002[2352] provided an exemption for "critical infrastructure information"[2353] that had been "voluntarily submitted."[2354] Unable to claim this exemption under the new mandatory reporting scheme,[2355] they in particular benefited from the presumption of confidentiality provided by the FCC Outage Reporting Rule.

FCC's decision to not routinely disclose outage reporting information was met with criticism by security experts,[2356] consumer advocates,[2357] and state regulators.[2358]

[2351] FCC Report and Order and Further Notice of Proposed Rule Making, FCC 04-188, ET Docket No. 04-35, Aug. 19, 2004, at 5.

[2352] Subtitle B of Title II of the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002) (codified at 6 U.S.C. §§ 131-34). *Cf.* NAT'L ACAD. OF ENG'G, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES 25 et seq. (Stewart D. Personick & Cynthia A. Patterson eds., 2003) (discussing why the Freedom of Information Act was perceived as a barrier to the sharing of critical infrastructure information).

[2353] *See* 6 U.S.C. § 131(3) (defining "critical infrastructure information" as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems […]").

[2354] *See* 6 U.S.C. § 133(a)(1)(A). *Cf.* 6 U.S.C. § 131(7) (defining voluntary submission of critical infrastructure information as "the submittal thereof in the absence of [a covered Federal] agency's exercise of legal authority to compel access to or submission of such information […]").

[2355] *Cf.* Christopher Guttman-McCabe et al, *Homeland Security and Wireless Telecommunications: The Continuing Evolution of Regulation*, 57 FED. COMM. L.J. 413, 446 (2005) (noting that mandatory reporting had a significant impact on the wireless industry, in particular because by requiring data collection, the information would automatically fall outside of the Critical Infrastructure Information Act of 2002).

[2356] *See, e.g.,* Bruce Schneier, *The Non-Security of Secrecy*, COMMUNICATIONS OF THE ACM, Oct. 2004, at 120, 120, *available at* http://www.schneier.com/essay-056.html (arguing that secrecy prevents people from assessing their own risks while public reporting of network outages forces telephone companies to improve their service); Bob Sullivan, *Why cell phone outage reports are secret*, MSNBC.COM, Dec. 15, 2006, http://redtape.msnbc.com/2006/12/why_cell_phone_.html (stating that Roger Cressey, former chief of staff of the President's Critical Infrastructure Protection Board could not imagine a scenario where the reports would be valuable to terrorists and further quoting Cressey: "it is corporate competition protection").

[2357] *See* Christopher Stern, *FCC Cuts Public Line To Phone Outage Data*, WASH. POST, Aug. 28, 2004, at E01 (noting that "[l]arge companies use the information to make decisions about where they build their own networks and to plan for key facilities such as data centers"). *See also* Caron Carlson, *Is Network Outage*

In November 2009, The California Public Utilities Commission (CPUC) filed a Petition for Rulemaking[2359] requesting that the FCC at least grant State public utilities commissions direct access to the FCC's Network Outage Reporting System (NORS) database.[2360] As of early November 2010, the FCC has not yet decided on the issue.

6.3.1.6. Enforcement

If a communications provider willfully[2361] or repeatedly[2362] fails to comply with the FCC Outage Reporting Rule, the FCC may issue a Notice of Apparent Liability for Forfeiture pursuant to § 503(b)[2363] of the Communications Act. The provider will then have a reasonable period of time (usually 30 days) to show, in writing, why a forfeiture penalty should not be imposed or should be reduced, or to pay the forfeiture.[2364] If the proposed forfeiture penalty is not paid in full in response to the notice of apparent liability, the FCC will issue an order canceling or reducing the proposed forfeiture or requiring that it be paid in full.[2365] If the

Information a Terror Threat?, EWEEK.COM, Oct. 4, 2004, http://www.eweek.com/c/a/Government-IT/Is-Network-Outage-Information-a-Terror-Threat.

[2358] *See* Christopher Stern, *FCC Cuts Public Line To Phone Outage Data*, WASH. POST, Aug. 28, 2004, at E01. *Cf. also* MINORITY STAFF OF H.R. COMM. ON GOV'T REFORM, 108TH CONG., SECRECY IN THE BUSH ADMINISTRATION 25 (2004), *available at* http://www.fas.org/sgp/library/waxman.pdf.

[2359] Petition of the California Public Utilities Commission and the People of the State of California for Rulemaking on States' Access to the Network Outage Reporting System (NORS) Database and a Ruling Granting California Access to NORS, ET Docket No. 04-35 (Nov. 12, 2009).

[2360] *See* http://www.fcc.gov/pshs/services/cip/nors/nors.html (last accessed Feb. 10, 2011).

[2361] *See* Communications Act of 1934 § 312(f)(1), 47 U.S.C. 312(f)(1) (defining "willful" as "the conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate").

[2362] *See* Communications Act of 1934 § 312(f)(2), 47 U.S.C. 312(f)(2) (defining "repeated" as "the commission or omission of [any] act more than once or, if such commission or omission is continuous, for more than one day").

[2363] 47 U.S.C. § 503(b).

[2364] *See* 47 C.F.R. § 1.80(f)(3).

[2365] *See* 47 C.F.R. § 1.80(f)(4).

forfeiture is not paid, the case will be referred to the Department of Justice which has to enforce the forfeiture order by bringing a civil suit against the provider.[2366]

6.3.2. The EU Telecoms Framework Directive

In EU law, Parliament and Council Directive 2002/21[2367] (hereinafter *Telecoms Framework Directive*) implements a network security breach notification policy. This policy was introduced into the Telecoms Framework Directive by Parliament and Council Directive 2009/140[2368] (hereinafter *Better Regulation Directive* or *BRD*) which was adopted as part of the "Telecoms Package"[2369] and has to be transposed by Member States by May 25, 2011.[2370]

6.3.2.1. The Notification Regime's Scope of Application

Article 13a(3) of the Telecoms Framework Directive as amended by the BRD requires undertakings "providing public communications networks" or "publicly available electronic communications services" to notify the competent national regulatory authority of "a breach of security or loss of integrity that has had a significant impact on the operation of networks or services."[2371]

[2366] *See* Communications Act of 1934 § 504(a), 47 U.S.C. § 504(a). *See also* 47 C.F.R. § 1.80(f)(5).

[2367] 2002 O.J. (L 108) 33 (EC).

[2368] 2009 O.J. (L 337) 37 (EC).

[2369] This legislative package consists of three legal acts: the Better Regulation Directive, Parliament and Council Directive 2009/136, 2009 O.J. (L 337) 11 (EC), and Parliament and Council Regulation 1211/2009, 2009 O.J. (L 337) 1 (EC).

[2370] *See* BRD art. 5.

[2371] Telecoms Framework Directive art. 13a(3). Note that in contrast to ePrivacy Directive art. 4(3), the personal scope of application of Telecoms Framework Directive art. 13a(3) covers not only "providers of publicly available electronic communications services" but also "providers of public communications networks." *Cf. supra* chapter 6.2.9 (discussing the ePrivacy Directive's data security breach notification regime).

The notification regime's material scope of application covers any "breach of security" as well as any "loss of integrity." This terminology is unfortunate since "security" is generally understood as encompassing confidentiality, integrity, and availability,[2372] which would make any "loss of integrity" also a "breach of security." Article 13a(1) and (2) shed some light on the reasons for using two different terms[2373]:

Article 13a(2) of the Telecoms Framework Directive mandates that providers of public communications networks "take all appropriate steps to guarantee the *integrity of their networks*, and thus ensure the continuity of supply of services provided over those networks."[2374]

According to article 13a(1) of the Telecoms Framework Directive, both types of covered providers—providers of public communications networks as well as providers of publicly available electronic communications services—are required to "take […] measures to appropriately manage the risks posed to *security of networks and services*."[2375]

It can be inferred from these provisions that the term "loss of integrity" only concerns communications networks while the term "breach of security" concerns both communications networks and communications services.[2376]

[2372] *See supra* chapter 2.1.

[2373] *See* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 46-47 (2010) (F.R.G.).

[2374] Telecoms Framework Directive art. 13a(2) (emphasis added).

[2375] Telecoms Framework Directive art. 13a(1) (emphasis added).

[2376] *See also* BRD recital 45 (stating that providers have to take "the necessary […] measures to appropriately manage risk to *security of networks and services* or to ensure the *integrity of their networks*" (emphasis added)). *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 47 (2010) (F.R.G.).

Even more important for determining what constitutes a "loss of [network] integrity" or a "breach of [network or service] security," Telecoms Framework Directive article 13a(3) only requires a network security breach notification if the incident "has had a significant impact on the *operation* of networks or services."[2377] This makes clear that both terms are intrinsically linked with the availability of communications capability. On the other hand, the confidentiality[2378] or integrity[2379] of communications is not a concern.[2380]

6.3.2.2. Notification of the Competent National Regulatory Authority

Article 13a(3) Telecoms Framework Directive requires the covered providers to notify any "breach of security" as well as any "loss of integrity" to the "competent national regulatory authority."[2381]

Remarkably, the wording of the Telecoms Framework Directive does not establish a time frame within which the regulatory authority has to be notified.[2382] Quarterly or even yearly notifications might therefore be sufficient to fulfill the Directive's requirements. Furthermore,

[2377] Telecoms Framework Directive art. 13a(3) (emphasis added).

[2378] For example, if an attacker managed to gain full access to a router operated by a provider, the attacker could eavesdrop on the users' communications but would not impact the "operations" of the network.

[2379] For example, if an attacker gained full access to a proxy server operated by a provider, the attacker could inject malicious code into the communications, compromising the integrity of communications. This would, however, not impact the "operations" of the network.

[2380] *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 47 (2010) (F.R.G.).

[2381] Telecoms Framework Directive art. 13a(3).

[2382] *Cf. supra* chapter 6.2.9 (discussing ePrivacy Directive art. 4(3) which requires that data security breach be notified to the competent national authority "without undue delay").

the Telecoms Framework Directive also does not establish any requirements regarding the content of a notification.[2383]

Once a national regulatory authority has been notified of a network security breach, it shall, "[w]here appropriate," inform the national regulatory authorities in other Member States as well as the European Network and Information Security Agency (ENISA).[2384] At a minimum, national regulatory authorities are required to once a year submit a summary report to the Commission and ENISA on the notifications received and the regulatory action taken in accordance with article 13a(3).[2385]

6.3.2.3. Notification of the Public

The Telecoms Framework Directive does not put national regulatory authorities under any obligation to notify the public.[2386] Under the Directive, a national regulatory authority "may" inform the public or require the provider to do so, "where it determines that disclosure of the breach is in the public interest."[2387] However, the Telecoms Framework Directive fails to provide any guidance regarding the criteria of this determination, making it likely that Member States will take very different approaches toward notifications of the public. Such

[2383] *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 47 (2010) (F.R.G.).

[2384] *See* Telecoms Framework Directive art. 13a(3). *Cf.* Parliament and Council Regulation 460/2004, 2004 O.J. (L 77) 1 (EC) (establishing the European Network and Information Security Agency). *See also* http://www.enisa.europa.eu (last accessed Feb. 10, 2011).

[2385] *See* Telecoms Framework Directive art. 13a(3).

[2386] Also note that national legislation regarding the right of access to documents (referred to as freedom of information in the U.S.) differs significantly from Member State to Member Sate. *Cf.* HERKE KRANENBORG & WIM VOERMANS, ACCESS TO INFORMATION IN THE EUROPEAN UNION: A COMPARATIVE ANALYSIS OF EC AND MEMBER STATE LEGISLATION (2005); EUROPEAN COMM'N, COMPARATIVE ANALYSIS OF THE MEMBER STATES' AND CANDIDATE COUNTRIES' LEGISLATION CONCERNING ACCESS TO DOCUMENTS (2003), *available at* http://ec.europa.eu/transparency/access_documents/docs/compa_en.pdf.

[2387] Telecoms Framework Directive art. 13a(3).

inconsistencies between national regulation are contrary to the BRD's stated purpose of "complet[ing] the internal market for electronic communications."[2388]

6.3.2.4. Notification Circumstances, Format, And Procedures

The Commission is empowered by the Telecoms Framework Directive to adopt[2389] "technical implementing measures" to harmonize national regulations adopted pursuant to article 13a(3), including measures defining the "circumstances, format and procedures applicable to notification requirements."[2390]

To prevent inconsistencies between national regulations, the Commission should at least resolve the following two questions: (1) What is the timeframe within which a provider has to notify the national regulatory authority? and (2) Under which circumstances should the national regulatory authority inform the public?[2391]

6.3.2.5. Enforcement

Article 21a of the Telecoms Framework Directive generally requires Member States to "lay down rules on penalties applicable to infringements of national provisions adopted pursuant to [the Directive]." These penalties must be "appropriate, effective, proportionate and

[2388] BRD recital 2 (also noting that "[i]n particular, regulatory fragmentation and inconsistencies between the activities of the national regulatory authorities were found to jeopardise not only the competitiveness of the sector, but also the substantial consumer benefits from cross-border competition"). *Cf.* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 47 (2010) (F.R.G.).

[2389] *See* Telecoms Framework Directive art. 13a(4) (stating that the implementing measures must be adopted in accordance with the "regulatory procedure with scrutiny" provided for in Council Decision 1999/468, art. 5a, 1999 O.J. (L 184) 23 (EC), as amended. *Cf.* BRD recitals 75 and 76.

[2390] Telecoms Framework Directive art. 13a(4).

[2391] *See* Lukas Feiler, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43, 47 (2010) (F.R.G.).

dissuasive."[2392] Additionally, competent national regulatory authorities shall have "the power to issue binding instructions"[2393] and "all the powers necessary to investigate cases of non-compliance."[2394]

6.3.3. Comparative Assessment

In the following, the two network security breach notification regimes implemented by the FCC Network Outage Reporting Rule and the Telecoms Framework Directive are comparatively assessed.

6.3.3.1. Policy Objectives

The policy objectives of network security breach notification can be three-fold: (1) enabling the public regulatory authority to perform risk mitigation by taking immediate reactive measures against the reported outage;[2395] (2) generally informing the public regulatory authority so that it can make better regulatory risk treatment decisions in the future,[2396] or (3) enabling informed risk decisions by (potential) subscribers which may ultimately result in an indirect risk transfer.[2397]

[2392] Telecoms Framework Directive art. 21a.

[2393] Telecoms Framework Directive art. 13b(1).

[2394] Telecoms Framework Directive art. 13b(3).

[2395] In 1992, the FCC stated that one of its purposes in requiring notification was "[t]o become aware of significant outages at the earliest possible time so that we may monitor developments [and] take immediate steps, as needed." *See* 57 Fed. Reg. 7,883, 7,884 (Mar. 5, 1992).

[2396] In 1992, the FCC stated that one of its purposes in requiring notification was, "after analyzing the information submitted, to determine what, if any, other action is required." *See id.*

[2397] In 1992, the FCC hinted at this objective by stating that one of its purposes in requiring notification was "to serve as a source of information for the public, to encourage and, where appropriate, to assist in dissemination of information to those affected." *See id.*

While the old FCC rules introduced in 1992 pursued all three policy objectives,[2398] the FCC Network Outage Reporting Rule as it is currently in force exclusively pursues the first two policy objectives.

The Telecoms Framework Directive only allows—but does not require—national regulatory authorities to inform the public or order the provider to do so. It therefore does not clearly pursue the third policy objective of enabling informed risk decisions by (potential) subscribers. Since it does not require the notification of the regulatory authorities within any specific time frame,[2399] it is also not concerned with the first potential policy objective of enabling immediate reactive measures. Indeed, the Telecoms Framework Directive only pursues the second policy objective of generally informing public regulatory authorities.

The first two policy objectives, which are both risk mitigation measures, are of some importance since they improve a regulatory authority's knowledge over the industry it is supposed to regulate. The third policy objective may have far more significant long-term effects on the level of availability offered by communications service providers.

Currently, (potential) subscribers may only learn about network security breaches if they have experienced the breaches themselves or if the breaches have been reported in the media. The data available to subscribers is therefore incomplete and non-comparable. This means that subscribers cannot take security aspects into account when making their buying decisions. In turn, this means that communications providers only face very few risks as a result of the low levels of availability of their networks and services. The third policy objective of enabling

[2398] *See id.*

[2399] *See supra* chapter 6.3.2.2.

informed risk decisions by (potential) subscribers could result in a risk transfer that addresses this misalignment between risk and risk mitigation capability.

To fulfill its full potential, a network security breach notification policy should put a strong emphasis on informing subscribers, so as not only to make it easier for regulatory agencies to manage the problem of network and information security but also to address the fundamental challenges of uninformed risk decisions and the misalignment between risk and risk mitigation capability.

6.3.3.2. Personal Scope of Application

The Telecoms Framework Directive covers providers of public communications networks as well as providers of publicly available electronic communications services. In particular, this covers all Internet backbone providers and Internet access providers, including broadband providers.

The FCC Network Outage Reporting Rule, on the other hand, only applies to communications providers that offer voice and/or paging communications. Given that today's information society strongly relies on the security and, in particular, the availability of the Internet communications infrastructure, this rather limited scope seems inappropriate.

Irrespective of which of the three policy objective identified above are pursued by a network security breach notification regime, it should take the increasing importance of Internet communications into account and should cover all types of commercial Internet backbone providers and Internet access providers, including broadband.

6.3.3.3. Network Security Breaches Subject to Mandatory Reporting

The FCC Network Outage Reporting Rule defines a complex set of condition under which losses of availability (i.e. outages) have to be reported. However, there is one condition that effectively excludes a large number of significant outages: an outage has to last at least 30 minutes for it to fall under mandatory reporting. Judging solely from mandatory outage reports, a provider suffering daily 20 minute outages would seem to provide more availability than a provider which only suffers a single 40 minute outage per year. In contrast to these limitations of the FCC Network Outage Reporting Rule, the Telecoms Framework Directive generally covers all losses of network or service availability.

Since the effects of many short-term outages can be as serious as the effects of a single longer outage, a network security breach notification regime should not exclude short-term outages from mandatory reporting. Using metrics such as the number of affected users and the amount of bandwidth lost, reported outages can be weighted accordingly.

6.3.3.4. Content Requirements for Notifications

The FCC Network Outage Reporting Rule requires that notifications in particular include the date and time of the onset of the outage, a brief description of the problem, and the particular services and geographic areas affected by the outage. The Telecoms Framework Directive, on the other hand, does not establish any content requirements.

To be effective, a network security breach notification regime should establish a detailed set of notification content requirements which should at least include the following: (1) date and time of the onset of the outage, (2) duration of the outage, (3) the communications network or service affected, (4) the geographic areas affected (5) a description of the problem, and (6) the number of subscribers and the estimated number of users affected.[2400]

[2400] Note that these numbers can differ significantly because a single subscriber's account can be used by multiple users (e.g. the members of a household or the employees of a corporation).

6.3.3.5. Enforcement

Both the FCC Network Outage Reporting Rule and the Telecoms Framework Directive exclusively provide public enforcement mechanisms by generally calling for penalties if a provider does not comply with its notification obligations.

The effectiveness of enforcement would greatly benefit if providers were obligated to also notify subscribers of all outages. Since all outages will be noticed directly at least by some subscribers, they are generally best positioned to detect instances of non-compliance, that is, outages for which a provider did not provide a notification.

6.3.3.6. Conclusion

Network security breach notification could be used as means of addressing the fundamental challenge of uninformed risk decisions as well as the challenge of the misalignment between risk and risk mitigation capability as applied to communications service providers. However, the network security breach notification regimes currently implemented in U.S. federal and EU law only require a notification of the competent regulatory authorities and do not provide for a routine disclosure of breach reports.

To not only enable risk mitigation by informed regulatory action but to also perform a risk transfer by allowing (potential) subscribers to make informed risk decisions, a less secretive approach is needed. A corresponding policy proposal will be presented *infra* in chapter 9.3.1.

6.4. Prohibiting Deceptive Security Claims About Products and Services

The previous three chapters have discussed regulatory policies that mandate certain disclosures.[2401] This chapter addresses the importance of the accuracy of voluntarily disclosed information by discussing regulatory policies that prohibit deceptive security claims. Such policies are particularly suitable to address the fundamental challenge of uninformed risk decisions.[2402]

6.4.1. Federal Trade Commission Act

Federal Trade Commission Act (FTC Act)[2403] § 5(a)[2404] directs the Federal Trade Commission (FTC) to prevent any person, partnership, or corporation[2405] from using "unfair or deceptive acts or practices in or affecting commerce"[2406] or involving foreign

[2401] *See supra* chapter 6.1 (discussing mandatory vulnerability disclosure for publicly traded companies), chapter 6.2 (discussing data security breach notification), and chapter 6.3 (discussing network security breach notification).

[2402] *Cf. supra* chapter 2.4.3.

[2403] Federal Trade Commission Act of 1914, Pub. L. No. 63-203, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. §§ 41-58 (2010)). *Cf. supra* chapter 4.1.6 (discussing FTC Act § 5 in the connection with the mandatory implementation of "reasonable" security controls).

[2404] 15 U.S.C. § 45 (2010).

[2405] Banks, savings and loan institutions, federal credit unions, common air carriers, and certain entities covered by the Packers and Stockyards Act of 1921, 7 U.S.C. § 181 et seq. are generally not covered by FTC Act § 5. *See* 15 U.S.C. § 45(a)(2).

[2406] FTC Act § 5(a)(1), 15 U.S.C. § 45(a)(1).

commerce.[2407] Since this chapter is only concerned with issues related to transparency, the following discussion exclusively focuses on *deceptive* acts or practices.[2408]

An act or practice is considered deceptive if it is likely to (1) mislead consumers; and (2) affect consumers' behavior or decisions about a product or service.[2409] As of February 10, 2011, the FTC has brought fifteen cases for deceptive claims regarding the security of personal information,[2410] all of which where settled by consent orders or stipulated judgments.

[2407] The Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 (US SAFE WEB Act), Pub. Law. No. 109-455, § 3, 120 Stat. 3372, 3372 (2006) (codified at 15 U.S.C. § 45(a)(4)(A)) expanded the definition of "unfair or deceptive acts or practices" to include acts or practices involving foreign commerce that (1) cause or are likely to cause reasonably foreseeable injury within the United States"; or (2) "involve material conduct occurring within the United States." *Cf. generally* Michael A. Rabkin, *When Consumer Fraud Crosses the International Line: The Basis for Extraterritorial Jurisdiction Under the FTC Act*, 101 NW. U. L. REV. 293 (2007).

[2408] For a discussion of how the prohibition of unfair acts or practices, as interpreted by the FTC, impacts information security see *supra* chapter 4.1.6.

[2409] FTC, ADVERTISING AND MARKETING ON THE INTERNET: RULES OF THE ROAD 2 (2000), available at http://business.ftc.gov/sites/default/files/pdf/bus28-advertising-and-marketing-internet-rules-road.pdf. *See also* Letter from James C. Miller III, Chairman, FTC, to John D. Dingell, Chairman, Subcommittee on Oversight and Investigations, Committee on Energy and Commerce (Oct. 14, 1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm (entitled "FTC Policy Statement on Deception"); Cliffdale Associates, Inc., 103 F.T.C. 110 (1984), 1984 WL 565319, at *37. *Cf. Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 27, 32 (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission) (defining deceptive practices as "material representations or omissions that are likely to mislead consumers acting reasonably under the circumstances").

[2410] Rite Aid Corp., FTC File No. 072-3121 (July 27, 2010) (the company had disposed personal information in open dumpsters while publicly claiming that it "takes its responsibility for maintaining your protected health information in confidence very seriously [and] would like to assure you that we respect and protect your privacy"); Twitter, Inc., FTC File No. 092-3093 (June 24, 2010) (the company's privacy policy stated that Twitter "employ[s] administrative, physical, and electronic measures designed to protect your information from unauthorized access" while the authentication procedures for administrative access where indeed very weak); CVS Caremark Corp., FTC Docket No. C-4259 (Feb. 18, 2009) (the company had failed to implement a reasonable disposal process, risk management program, or employee training program while publicly claiming that "nothing is more central to our operations than maintaining the privacy of your health information"); Genica Corp., FTC Docket No. C-4252 (Feb. 5, 2009) (the company had stored personal information in an unencrypted form and had generally failed to employ reasonable measures to detect and prevent unauthorized access to personal information while stating in its privacy policy that it uses "state of the art […] encryption" and has "put in place privacy protection control systems designed to ensure that personal Customer data remains safe and private"); Premier Capital Lending, Inc., FTC File No. 072-3004 (June 11, 2008); U.S. v. ValueClick, Inc., No. CV08-01711 MMM RZx (C.D. Cal. 2008) (stipulated final judgment); Goal Financial, LLC, FTC File No. 072-3013 (Mar. 4, 2008); Life Is Good, Inc., FTC File No. 072-3046 (Jan. 17, 2008); Guidance Software, Inc., FTC File No. 062-3057 (Nov. 16, 2006); U.S. v. Choicepoint Inc., 1 06-CV-0198 (N.D. Ga. 2006) (stipulated final judgment); Petco Animal Supplies, Inc., FTC Docket No. C-4133 (Mar. 4, 2005); MTS Inc., d/b/a Tower Records/Books/Video, FTC Docket No. C-4110 (May 28, 2004); Guess?, Inc., FTC Docket No. C-4091, In these cases, the FTC alleged that the respective companies made explicit or implicit promises to take reasonable steps to protect sensitive consumer information, but because they allegedly failed to take such steps, their claims were deceptive. In its enforcement practice, the FTC primarily relies on public reports of security breaches to learn of companies that might not have implemented "reasonable"[2411] security controls.[2412] However, the occurrence of a breach is not sufficient evidence for a failure to implement reasonable controls, because, as the FTC notes, "breaches can happen […] even when a company has taken every reasonable precaution."[2413] Moreover, as demonstrated in an enforcement action against Microsoft, the occurrence of a breach is not necessary to establish that the implemented security controls were not "reasonable."[2414]

(July 30, 2003); Microsoft Corp., FTC Docket No. C-4069 (Dec. 20, 2002); Eli Lilly & Co., FTC Docket No. C-4047 (May 8, 2002). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last accessed Feb. 10, 2011).

[2411] The FTC recognizes that "that good security is an ongoing process of assessing and addressing risks and vulnerabilities." *Protecting our Nation's Cyber Space: Educational Awareness for the Cyber Citizen: Hearing Before the Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census of the H. Comm. on Government Reform*, 108th Cong. 14, 21 (2004) (statement of the Federal Trade Commission). The FTC's security requirements, as deduced from its enforcement actions, can therefore only be generalized as mandating policies, processes, and procedures adequate to the risk presented. *See* Janine S. Hiller et. al., *Due Diligence on the Run: Business Lessons Derived from FTC Actions to Enforce Core Security Principles*, 45 IDAHO L. REV. 283, 309 (2009) (noting that the FTC "therefore leave[s] many of the hard decisions about necessary security to the individual business"); Travis D. Breaux & David L. Baumer, *Legally "Reasonable" Security Requirements: A 10-year FTC Retrospective*, COMPUTERS & SECURITY (forthcoming 2011) (noting that "the obligations [imposed by the FTC] fall short of explaining *how* companies can ensure that the steps they have taken are consistent with the full extent of these obligations" (emphasis in original)). *Cf. supra* chapter 4.1.10.4 (discussing the difficulty of determining "reasonableness" with regard to security controls).

[2412] Almost all of the enforcement actions mentioned above where triggered by publicly reported security breaches. *Cf.* Joel B. Hanson, *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, 4 SHIDLER J. L. COM. & TECH. 11, 14 (2008) (noting that, "[g]enerally, the FTC has only alleged [a deceptive act or practice] when a business' information security has actually been breached and the breach led to the acquisition of personal information by unauthorized individuals").

[2413] *Protecting our Nation's Cyber Space: Educational Awareness for the Cyber Citizen: Hearing Before the Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census of the H. Comm. on Government Reform*, 108th Cong. 14, 19 (2004) (statement of the Federal Trade Commission).

[2414] *See* Microsoft Corp., FTC Docket No. C-4069 (Dec. 20, 2002). *Cf. also Protecting our Nation's Cyber Space: Educational Awareness for the Cyber Citizen: Hearing Before the Subcomm. on Technology, Information*

It has to be emphasized that personal information controllers are not the only actors in the information security landscape to which FTC Act § 5 applies. In particular software manufacturers that make security claims that do not match the level of security actually provided by their products[2415] generally also commit deceptive acts or practices. However, so far, the FTC has not brought any notable cases against software manufacturers for the misrepresentation of the security of their products.[2416]

The sanctions available for deceptive (or unfair) acts or practices include cease and desist orders issued by the FTC and a civil penalty of up to $10,000 for each knowing violation.[2417] A private right of action is not available.[2418]

Remarkably, in the above-cited enforcement actions for deceptive claims regarding the security of personal information, the FTC has not sought any civil penalties for violation of

Policy, Intergovernmental Relations and the Census of the H. Comm. on Government Reform, 108th Cong. 14, 20 (2004) (statement of the Federal Trade Commission).

[2415] For example, Google has claimed that, due to the security architecture of Google Chrome OS, users would not have "to deal with viruses, malware and security updates." Sundar Pichai, Vice President, Google Inc., *Introducing the Google Chrome OS*, OFFICIAL GOOGLE BLOG, July 7, 2009, http://googleblog.blogspot.com/2009/07/introducing-google-chrome-os.html. *Cf.* Grant Gross, *Google's OS Security Claims Called 'idiotic'*, PCWORLD, July 8, 2009, http://www.pcworld.com/businesscenter/article/168087/googles_os_security_claims_called_idiotic.html (quoting Bruce Schneier). Apple claims that its web browser "Safari" was designed "to be highly secure from day one." http://www.apple.com/safari/what-is.html (last accessed Feb. 10, 2011). In 2002, Oracle advertised its relational database management system Oracle9i with the slogan "Unbreakable. Can't break it. Can't break in." *See* Kevin Poulsen, *Breakable*, SECURITYFOCUS, Jan. 16, 2002, http://www.securityfocus.com/news/309.

[2416] The FTC has only brought cases against the manufacturers of spyware. *Cf.* Megan M. Engle, *Anti-Spyware Enforcement: Recent Developments*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 581, 585 et seq. (2008).

[2417] For a full discussion of the sanctions available under FTC Act § 5 see *supra* chapter 4.1.6.

[2418] *See, e.g.,* Holloway v. Bristol-Myers Corp., 485 F.2d 986, 988-89 (D.C. Cir. 1973) ("The Act nowhere purports to confer upon private individuals, either consumers or business competitors, a right of action to enjoin the practices prohibited by the Act or to obtain damages following the commission of such acts."); Jeter v. Credit Bureau, 760 F.2d 1168, 1174 n.5 (11th Cir. 1985) (noting that "a private right of action […] does not exist under the FTC Act").

FTC Act § 5.[2419] However, the settlement agreements typically require measures nearly identical to those mandated by the FTC Safeguards Rule[2420] to be implemented and maintained for twenty years.[2421]

6.4.2. Deceptive Acts and Practices under California and New York State Law

California Business and Professions Code § 17200 prohibits any "deceptive, untrue or misleading advertising" as a means of unfair competition.[2422] For any violation, the state's attorney general may bring an action for an injunction[2423] or for civil penalties.[2424] A private cause of action, that was independent of possible injuries suffered by the plaintiff, has been eliminated by Proposition 64[2425] which was passed in 2004.[2426] However, Proposition 64 did not eliminate competitor actions for injunctive relief.[2427]

[2419] However, if other statutes such as HIPAA or FCRA had also been violated, the FTC did seek civil penalties under those statutes. See, for example, U.S. v. Choicepoint Inc., 1 06-CV-0198 (N.D. Ga. 2006) where Choicepoint agreed to pay $10 million in civil penalties and $5 million to redress consumers who became victims of impersonation fraud and Rite Aid Corp., FTC File No. 072-3121 (July 27, 2010) where Rite Aid agreed to pay $1 million to settle allegations of HIPAA violations. *Cf. also* Joel B. Hanson, *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, 4 SHIDLER J. L. COM. & TECH. 11, 34-37 (2008).

[2420] *See supra* chapter 4.1.2.1 (describing the requirements under the FTC Safeguards Rule).

[2421] *See Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 27, 28 (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission) ("The consent orders […] have required the companies to implement appropriate information security programs that generally conform to the standards that the Commission set forth in the GLBA Safeguards Rule."). *Cf. also* Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, FED. LAW., Sept. 2007, at 39, *available at* 54-SEP Fed. Law. 39 (Westlaw) (criticizing the expansion of the personal scope of application of the FTC Safeguards Rule).

[2422] CAL. BUS. & PROF. CODE § 17200(a) (West 2010).

[2423] *See* CAL. BUS. & PROF. CODE § 17204.

[2424] *See* CAL. BUS. & PROF. CODE § 17206.

[2425] *See* 2004 Cal. Legis. Serv. Prop. 64 (West). CAL. BUS. & PROF. CODE § 17204 as amended by Proposition 64 provides that a person may only bring an action under CAL. BUS. & PROF. CODE § 17200 et seq. if she has actually "suffered injury in fact and has lost money or property as a result of the unfair competition." *See* Bivens v. Gallery Corp., 36 Cal. Rptr. 3d 541, 548 (2005), *reh'g denied*, 2005 Cal. App. LEXIS 2037 (Cal. Ct. App. 2006), *review granted*, *depublished*, 130 P.3d 518 (Cal. 2006), *review dismissed*, 154 P.3d 1001 (Cal. 2007). *Cf.* Sharon J. Arkin, *The Unfair Competition Law after Proposition 64: Changing the Consumer Protection*

Similarly, New York General Business Law § 349 prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in [the state of New York]."[2428] The state's attorney general may seek an injunction and a restitution of any moneys or property obtained by the deceptive acts or practices.[2429] A private cause of action is not available unless the plaintiff can show that he has been injured.[2430]

Under both California and New York law, courts have repeatedly denied standing to consumers who alleged that an increased risk of "identity theft"—or the costs associated with mitigating that risk—constituted an injury within the meaning of the law.[2431]

California and New York state attorneys general have used California Business and Professions Code § 17200 and New York General Business Law § 349 respectively to

Landscape, 32 W. ST. U. L. REV. 155 (2005); Jacquetta Lannan, *Saving 17200: An Analysis of Proposition 64*, 46 SANTA CLARA L. REV. 451 (2006); Christopher W. Arledge, *Standing Under the Unfair Competition Law is Unlikely to Exist for Competitors*, 50 ORANGE COUNTY LAW. 51 (2008).

[2426] *Cf.* CAL. CONST. art. II, § 8 (stating that "[t]he initiative is the power of the electors to propose statutes and amendments to the Constitution and to adopt or reject them").

[2427] *See* Clayworth v. Pfizer, Inc., 233 P.3d 1066, 1088 (Cal. 2010) (holding that the right to seek injunctive relief under CAL. BUS. & PROF. CODE § 17203 is not dependent on the right to seek restitution). *Cf. also* Finelite, Inc. v. Ledalite Architectural Prods., No. C-10-1276 MMC, 2010 WL 3385027 (N.D. Cal. Aug. 16, 2010) (applying *Clayworth*).

[2428] N.Y. GEN. BUS. LAW § 349(a) (McKinney 2010).

[2429] *See* N.Y. GEN. BUS. LAW § 349(b).

[2430] *See* N.Y. GEN. BUS. LAW § 349(h).

[2431] *See, e.g.,* Shafran v. Harley-Davidson, Inc., No. 07 CIV. 01365 (GBD), 2008 WL 763177, at *3 (S.D.N.Y. Mar. 20, 2008) ("Courts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy") (applying N.Y. state law); Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008), *aff'd*, 380 F. App'x. 689 (9th Cir. 2010) ("[Plaintiff's] attempt to allege that the theft of the laptops somehow constitutes a loss of property because his personal information was contained on the laptop is unavailing."); Hammond v. The Bank of New York Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *13 (S.D.N.Y. June 25, 2010) ("it is not surprising that the United States District Courts in New York, California, Illinois and Michigan (applying state law) have each found that the increased risk of identity theft (in the future) is not a cognizable claim" (applying N.Y. and California law)).

prosecute companies that had failed to implement security controls commensurate with their public security claims.[2432] However, such enforcement actions are rather rare.

6.4.3. EU Unfair Commercial Practices Directive

Parliament and Council Directive 2005/29[2433] (hereinafter *Unfair Commercial Practices Directive*) prohibits unfair commercial practices before, during and after a business-to-consumer[2434] commercial transaction in relation to a product or service.[2435] In particular, the Unfair Commercial Practices Directive prohibits "misleading commercial practices"[2436] which

[2432] *See, e.g.,* In re Eli Lilly, Inc., Assurance of Voluntary Compliance and Discontinuance (July 25, 2002), *available at* http://supplierportal.lilly.com/SiteCollectionDocuments/Multi_State_Order.pdf (entered into by the attorneys general of California, Connecticut, Idaho, Iowa, Massachusetts, New Jersey, New York, and Vermont). Eli Lilly represented in its privacy policy that it employs appropriate security measures; however, it sent out an e-mail to subscribers of its Prozac.com site and accidentally disclosed all other subscribers' e-mail addresses by using the "To" instead of the "Bcc" field. Eli Lilly agreed to implement reasonable security procedures and pay $160,000 to the eight states pursuing the action. *See also* Ziff Davis Media Inc., Assurance of Discontinuance (Aug. 28, 2002), *available at* http://www.ag.ny.gov/media_center/2002/aug/aug28a_02_attach.pdf (entered into by the attorneys general of the states of New York, California, and Vermont). Ziff Davis stated in its privacy policy that "[w]e use reasonable precautions to keep the personal information […] secure" but stored personal information of magazine subscribers in an unencrypted flat file that was publicly accessible without authentication. Ziff Davis agreed to implement specific security measures and to pay $100,000 to the three states and $500 to each consumer who submitted credit card information. *Cf.* Stephen F. Ambrose & Joseph W. Gelb, *Consumer Privacy Regulation, Enforcement, and Litigation in the United States*, 58 BUS. LAW. 1181, 1189 (2003); Kathryn E. Picanso, *Protecting Information Security Under A Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 367 (2006)

[2433] 2005 O.J. (L 149) 22 (EC).

[2434] *See* Unfair Commercial Practices Directive art. 2(a) (defining "consumer" as "any natural person who, in commercial practices covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession"). Note that Council Directive 84/450, art. 3, 1984 O.J. (L 250) 17, 18 (EEC) as amended by the Unfair Commercial Practices Directive contains an almost identical prohibition as that discussed *infra* which however (1) only applies to "advertising"; and (2) also applies in business-to-business relationships. *See generally* FRAUKE HENNING-BODEWIG, UNFAIR COMPETITION LAW: EUROPEAN UNION AND MEMBER STATES 36 et seq. (2006).

[2435] *See* Unfair Commercial Practices Directive art. 5(1) (prohibiting "unfair commercial practices"), art. 3(1) (stating that the Directive shall apply to transaction "in relation to a product"), art. 2(c) (defining "products" as "any goods or service including immovable property, rights and obligations").

[2436] *See* Unfair Commercial Practices Directive art. 5(4)(a) in conjunction with art. 6. Another type of unfair commercial practices not discussed here are aggressive commercial practices. Unfair Commercial Practices Directive art. 5(4)(b) in conjunction with art. 8 and 9. For a general discussion of the Unfair Commercial Practices Directive see Giuseppe B. Abbamonte, *The Unfair Commercial Practices Directive: An Example of the New European Consumer Protection Approach*, 12 COLUM. J. EUR. L. 695 (2006).

includes any practice that (1) contains false information or in any way deceives or is likely to deceive the average consumer[2437] about, *inter alia*, "the main characteristics of the product, such as its benefits, risks, [...] fitness for purpose, [...] specification, [...] or the results to be expected from its use, or the results and material features of tests or checks carried out on the product";[2438] and (2) causes or is likely to cause the consumer to take a transactional decision that he would not have taken otherwise.[2439]

Furthermore, the Unfair Commercial Practices Directive prohibits, irrespective of a likelihood of deception or influence of the consumer, certain misleading practices set out in an exhaustive[2440] list in annex I of the Directive. As regards information security, the most relevant of these practices is to claim that "a product has been approved, endorsed or authorised by a public or private body when [it] has not or making such a claim without complying with the terms of the approval, endorsement or authorization"[2441] (e.g. falsely claiming to have obtained a Common Criteria certification for a product).[2442]

[2437] *See* Unfair Commercial Practices Directive art. 6(1) ("Misleading actions"). Another type of misleading commercial practices not discussed here are misleading omissions. *See* Unfair Commercial Practices Directive art. 7.

[2438] Unfair Commercial Practices Directive art. 6(1)(b).

[2439] *See* Unfair Commercial Practices Directive art. 6(1). Note that Council Directive 84/450, art. 3, 1984 O.J. (L 250) 17, 18 (EEC) as amended by the Unfair Commercial Practices Directive contains an almost identical prohibition which however (1) only applies to "advertising"; and (2) also applies in business-to-business relationships. *See generally* FRAUKE HENNING-BODEWIG, UNFAIR COMPETITION LAW: EUROPEAN UNION AND MEMBER STATES 36 et seq. (2006).

[2440] *See* Case C-304/08, Zentrale zur Bekämpfung unlauteren Wettbewerbs eV v Plus Warenhandelsgesellschaft mbH, 2010 E.C.R. I-0000, § 45; Joined Cases C-261/07 and C-299/07, VTB-VAB NV v. Total Belgium NV, 2009 E.C.R. I-02949, § 43. *See also* Unfair Commercial Practices Directive recital 17 (stating with regard to annex I that "[t]hese are the only commercial practices which can be deemed to be unfair without a case-by-case assessment against the provisions of Articles 5 to 9").

[2441] Unfair Commercial Practices Directive annex I.4.

[2442] *See supra* chapter 4.5.4.2 (discussing product certifications under the Common Criteria).

The Unfair Commercial Practices Directive clearly also applies to providers of communications services,[2443] providers of online services, software manufacturers, or software sellers.[2444] Accordingly, misleading statements made by any of these actors about the security of their products or services, is prohibited under the Directive and is to be sanctioned by "effective, proportionate and dissuasive" penalties.[2445] Furthermore, Member States had to adopt provisions under which competitors and other "persons or organisations regarded under national law as having a legitimate interest" (this does not necessarily include consumers) may take legal action against unfair commercial practices and/or bring such practices before an administrative authority.[2446]

However, so far no cases have been reported in which a national legislation that was adopted to transpose the Unfair Commercial Practices Directive had been used against companies who made misleading statements about the levels of information security offered by their products or services.

6.4.4. Comparative Assessment

Companies typically provide little security-related information about their products or services on a voluntary basis. Therefore it is all the more important that the information that is disclosed is indeed accurate. A regulatory policy that attempts to enforce such accuracy by prohibiting deceptive statements about the levels of information security offered by products

[2443] *Cf., e.g.,* Case C-522/08, Telekomunikacja Polska SA w Warszawie v. Prezes Urzędu Komunikacji Elektronicznej, 2010 E.C.R. I-0000 (applying the Unfair Commercial Practices Directive to a provider of a publicly available electronic communications service).

[2444] *See* Unfair Commercial Practices Directive art. 2(1) (defining "product" as "any goods or service including immovable property, rights and obligations," thereby in particular also covering software license agreements).

[2445] *See* Unfair Commercial Practices Directive art. 13.

[2446] *See* Unfair Commercial Practices Directive art. 11(1).

or services is a significant instrument to address the fundamental challenge of misinformed or, more generally uninformed risk decisions.[2447]

All of the regulatory instruments discussed above clearly prohibit deceptive security claims. Despite the fact that none of them grants standing to a consumer if he cannot prove injury, they generally provide adequate enforcement mechanisms. There is, however, one remarkable difference when comparing the situation in the EU and the U.S.: There have been considerably more efforts in the U.S. to use unfair competition statutes in reaction to a security breach.[2448]

This difference in enforcement practices can be attributed to two factors directly related to a differing general legal situation in the U.S.: First, there are numerous security breach notification regimes under U.S. law[2449] which essentially ensure that a high number of security breaches comes to the attention of the FTC and the attorneys general of the relevant states. In the EU, on the other hand, few if any obligations exist to notify security breaches.[2450]

Second, websites in the U.S. typically post a privacy policy; in many cases because they are obligated to do so.[2451] This means that the FTC and the state attorneys general in many cases

[2447] *See supra* chapter 2.4.3.

[2448] *See supra* chapters 6.4.1 and 6.4.2 (referring to numerous enforcement actions under the FTC Act and under California and New York state law).

[2449] *See supra* chapters 6.2.1 to 6.2.8.

[2450] *See* chapter 6.2.9 (discussing breach notification under ePrivacy Directive art. 4(3) which has to be transposed by Member States until May 25, 2011).

[2451] Under California law "[a]n operator of a commercial Web site […] that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site […] shall conspicuously post its privacy policy on its Web site." CAL. BUS. & PROF. CODE § 22575(a). There is no such obligation under New York state law. However website operators covered by have public statements from companies promising to implement reasonable measures that, if they had been implemented, would have prevented the breach. On the other hand, EU law puts website operators under no obligation to post a privacy policy, leading to a situation where few websites actually have one. This means that even if public authorities learn of a security breach—which is rarely the case, given the general lack of an obligation to notify breaches—they often have no public statements of the company in question, promising any specific level of information security. Indeed, from a legal perspective, such a statement would be largely redundant because the national laws adopted pursuant to the Data Protection Directive already impose significant obligations on all website operators,[2452] rendering most self-imposed restrictions superfluous. However, the difference is that under the Unfair Commercial Practices Directive, a violation of statutory law does not by itself constitute an unfair commercial practice.[2453]

It is likely that for these reasons, unfair competition statutes have been used to a much greater extent in the U.S. than in the EU to prosecute companies that have suffered a security breach.

GLBA, HIPAA, or COPPA generally have to post a privacy policy. *See* 15 U.S.C. § 6803; 45 C.F.R. § 164.520; 15 U.S.C. § 6502(b)(1)(A)(i).

[2452] *See supra* chapter 4.1.8 (discussing the security requirements under the Data Protection Directive).

[2453] A violation of statutory law only constitutes an unfair commercial practice under the Directive if it falls within the general prohibition of art. 5(2), that is if it (a) "is contrary to the requirements of professional diligence"; and (b) "materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers." *Cf. generally* Giuseppe B. Abbamonte, *The Unfair Commercial Practices Directive: An Example of the New European Consumer Protection Approach*, 12 COLUM. J. EUR. L. 695, 704 et seq. (2006).

7. Regulating Information Security by Deterring Malicious Threat Agents

Another regulatory approach to information security is to attempt to deter malicious threat agents by imposing criminal sanctions.[2454] This approach focuses on the threat agent component of a risk.[2455]

Attacks on the security of information potentially come within the scope of a wide array of criminal statutes.[2456] However, the following chapters will only focus on those statutes that are of most importance in practice. Since most information is today stored, processed, and transmitted in electronic form,[2457] it is no coincidence that the statutes discussed *infra* all focus on attacks against computers and computer networks.

7.1. Federal Computer Crime Law

The following federal computer crime statutes are discussed below: the Computer Fraud and Abuse Act (see *infra* chapter 7.1.1), the Wiretap Act (see *infra* chapter 7.1.2), and the Stored Communications Act (see *infra* chapter 7.1.3).

[2454] In addition to criminal sanctions, civil liability potentially also has a deterrent effect on malicious threat agents. However, that deterrent effect—when compared to criminal sanctions—is negligible, in particular because it is even more difficult to identify the perpetrator for the victim than it is for law enforcement agencies. Accordingly, this thesis will exclusively focus on criminal law.

[2455] *Cf. supra* chapter 3.1 (defining the components of information security risks).

[2456] For example, for a discussion of crimes related to those established under the Computer Fraud and Abuse Act see CHARLES DOYLE, CONG. RESEARCH SERV., CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS, CRS REPORT FOR CONGRESS NO. 97-1025 (2008), *available at* http://www.fas.org/sgp/crs/misc/97-1025.pdf.

[2457] *Cf. supra* chapter 1 (discussing the relation between information security and IT security).

7.1.1. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act[2458] (hereinafter *CFAA*) is a federal statute that criminalizes certain behavior set out in 18 U.S.C. § 1030(a)(1)-(7).[2459] At the outset it should be noted that many of the CFAA's provisions only apply to "protected computers."[2460] This term is defined as a computer which (1) is exclusively for the use of a financial institution or the United States Government; (2) is non-exclusively used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (3) is used in or affecting interstate or foreign commerce or communication.[2461] As regards computers located in the U.S., the latter alternative has been interpreted very broadly, effectively covering any computer connected to the Internet.[2462]

Section 1030(a)(1) outlaws the disclosure or retention of sensitive government information[2463] obtained by knowingly accessing[2464] a computer without authorization[2465] or exceeding

[2458] Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified at 18 U.S.C. § 1030 as amended).

[2459] Conspiring to commit or attempting to commit any of the offenses under § 1030(a)(1)-(7) is also covered by the CFAA. 18 U.S.C. § 1030(b) (2010).

[2460] *See* 18 U.S.C. §1030(a)(2)(C), (a)(4), (a)(5), and (a)(7).

[2461] 18 U.S.C. § 1030(e)(2).

[2462] *See* United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (holding that, with a connection to the Internet, the victim's computers that were located in Missouri were part of a system that is inexorably intertwined with interstate commerce and thus protected under 18 U.S.C. § 1030, irrespective of the victim organization's not-for-profit status). *Cf. also* MARK G. MILONE, INFORMATION SECURITY LAW: CONTROL OF DIGITAL ASSETS § 9.01[1] (2009). Computers located outside the U.S. are also covered if they are "used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B).

[2463] This only covers information "that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954." 18 U.S.C. § 1030(a)(2).

[2464] "Accessing" a computer has been interpreted broadly and in particular covers visiting a website. *Cf., e.g.,* Sw. Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004) (holding with regard to authorization[2466] if the offender has reason to believe that the information could be used to the injury of the United States, or to the advantage of any foreign nation.[2467] This effectively criminalizes espionage activities that are carried out by accessing a computer without (sufficient) authorization. Violations are punishable by imprisonment for not more than ten years[2468] (not more than twenty years for second and subsequent offenses)[2469] and a fine of not more than $250,000.[2470]

Subsection (a)(2) prohibits intentionally accessing a computer without (sufficient) authorization thereby obtaining (a) certain financial information;[2471] (b) information from any department or agency of the United States; or (c) information from any protected computer.[2472] Violations are punishable by imprisonment for not more than one year and a

§ 1030(a)(2) that accessing fare and scheduling information that Southwest publishes on Southwest.com is covered by the CFAA). For a critical perspective see Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

[2465] *Cf.* eBay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) (holding with regard to § 1030(a)(2) that "[a]llegations with respect to access and use beyond those set forth in a user agreement constitute unauthorized use under the CFAA"). Note that it is sufficient that the offender knows that he is not authorized to access a computer (in a certain way); an enforceable contract prohibiting (certain ways of) access is not required. *See* Sw. Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004) (holding that it is not material whether a website's use agreement creates an enforceable contract; it is sufficient that the offender knew that the alleged uses were prohibited).

[2466] This also covers instances where the offender uses his access privileges in an unauthorized manner or for unauthorized purposes. *Cf.* YourNetDating, Inc. v. Mitchell, 88 F. Supp. 2d 870, 872 (N.D. Ill. 2000) (finding with regard to § 1030(a)(2) that a former employee accessed a computer exceeding authorization because he used his administrative access to divert users from his ex-employers website).

[2467] 18 U.S.C. § 1030(a)(1).

[2468] 18 U.S.C. §§ 1030(c)(1)(A).

[2469] 18 U.S.C. §§ 1030(c)(1)(B).

[2470] 18 U.S.C. § 3571(b)(3).

[2471] This covers information contained in (a) a financial record of a financial institution, or of a card issuer or (b) a file of a consumer reporting agency on a consumer. 18 U.S.C. § 1030(a)(2)(A).

[2472] 18 U.S.C. § 1030(a)(2).

fine of not more than $100,000.[2473] (not more than five years and a fine of not more $250,000 in aggravated cases[2474] and not more than ten years for second and subsequent offenses[2475]).

Subsection (a)(3) criminalizes intentionally accessing a nonpublic federal government computer "without authorization."[2476] It also covers computers used non-exclusively by the federal government if the conduct affects that use.[2477] Violations are punishable by imprisonment for not more than one year and a fine of not more than $100,000[2478] (not more than ten years and not more than $250,000 for second and subsequent offenses).[2479]

Subsection (a)(4) outlaws knowingly and with intent to defraud, accessing a protected computer without (sufficient) authorization, thereby furthering a fraud and obtaining anything of value other than computer time worth less than $5,000 in any one-year period. Such computer fraud is punishable by imprisonment for not more than five years[2480] (not more than ten years for second and subsequent offenses)[2481] and a fine of not more than $250,000.[2482]

[2473] 18 U.S.C. §§ 1030(c)(2)(A), 3559(a)(6), 3571(b)(5).

[2474] 18 U.S.C. §§ 1030(c)(2)(B), 3571(b)(3). This applies if the value of the information obtained exceeds $5,000 or if the offense was committed in furtherance of any criminal or tortious act or for purposes of commercial advantage or private financial gain. *Id.*

[2475] *See* 18 U.S.C. § 1030(c)(2)(C).

[2476] 18 U.S.C. § 1030(a)(3). Note that this provision does not cover access that merely exceeds authorization, thereby "limit[ing] 18 U.S.C. 1030(a)(3) to cases where the offender is completely outside the Government, and has no authority to access a computer of any agency or department of the United States, or where the offender's act of trespass is interdepartmental in nature." S. REP. NO. 99-432, at 7-8 (1986).

[2477] *Id.*

[2478] 18 U.S.C. §§ 1030(c)(2)(A), 3559(a)(6), 3571(b)(5).

[2479] *See* 18 U.S.C. §§ 1030(c)(2)(C), 3571(b)(3).

[2480] 18 U.S.C. § 1030(c)(3)(A).

[2481] 18 U.S.C. § 1030(c)(3)(B).

[2482] 18 U.S.C. § 3571(b)(3).

Subsection (a)(5) establishes three offenses based on the causation of damage to a protected computer: (1) knowingly causing the transmission of any data or code, thereby intentionally causing damage without authorization, to a protected computer;[2483] (2) intentionally accessing a protected computer without authorization, thereby recklessly causing damage;[2484] and (3) intentionally accessing a protected computer without authorization, thereby causing (whether intentionally, recklessly, or otherwise) damage and loss.[2485] It should be noted that "damage" which is defined by the statute as "any impairment to the integrity or availability of data, a program, a system, or information"[2486] has been construed by the courts very liberally so as to also include the disclosure of information even though "no data was physically changed or erased."[2487] Section 1030 provides more severe punishment for the first offense (intentional causation of damage) than for the second (reckless causation) or third offense (unqualified causation), ranging from a term of imprisonment of not more than one year and a fine of not

[2483] 18 U.S.C. § 1030(a)(5)(A). Note that this does not require that the offender accesses the protected computer. *See* S. REP. NO. 104-357, at 10 (1996) (stating that "[t]his would cover anyone who intentionally damages a computer, regardless of whether they were an outsider or an insider otherwise authorized to access the computer"). *See also* In re Am. Online, Inc., 168 F. Supp. 2d 1359, 1371 (S.D. Fla. 2001). *Cf.* U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 32 (2007), *available at* http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf (noting that "it is possible to damage a computer without 'accessing' it [...]. For example, most worms and trojans spread though self-replication, without personally accessing the affected systems.").

[2484] 18 U.S.C. § 1030(a)(5)(B).

[2485] 18 U.S.C. § 1030(a)(5)(C). *Cf.* 18 U.S.C. § 1030(e)(11) (defining "loss" broadly as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service").

[2486] 18 U.S.C. § 1030(e)(8).

[2487] Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000); Therapeutic Research Faculty v. NBTY, Inc., 488 F. Supp. 2d 991, 996 (E.D. Cal. 2007). Given that availability and integrity (which are both mentioned by the statute) are typically recognized as distinct from confidentiality (*cf. supra* chapter 2.1), this liberal construction of § 1030(a)(5) is indeed questionable.

more than $100,000 to not more than twenty years or even life in the case of the reckless causation of death.[2488]

Subsection (a)(6) criminalizes knowingly trafficking, with the intent to defraud, in any password or similar information[2489] through which a computer may be accessed without authorization if such trafficking affects interstate or foreign commerce or such computer is used by or for the federal government.[2490] Such trafficking in computer access information is punishable by imprisonment for not more than one year and a fine of not more than $100,000[2491] (not more than ten years and not more than $250,000 for second and subsequent offenses).[2492]

Lastly, subsection (a)(7) outlaws transmitting any communication in interstate or foreign commerce with the intent to extort anything of value if the transmission contains (A) a threat to cause damage to a protected computer; (B) a threat to obtain information from a protected computer without (sufficient) authorization or to impair the confidentiality of information

[2488] Violations of the first offense established by subsection (a)(5) are punishable by imprisonment of not more than one year and a fine of not more than $100,000 (18 U.S.C. §§ 1030(c)(4)(G), 3559(a)(6), 3571(b)(5)); if the offense caused certain harms, in particular "damage affecting 10 or more protected computers during any 1-year period" (18 U.S.C. § 1030(c)(4)(A)(I)-(VI)), not more than ten years and a fine of not more than $250,000 (18 U.S.C. §§ 1030(c)(4)(B), 3571(b)(3)); if the offender attempts to cause or knowingly or recklessly causes serious bodily injury (18 U.S.C. §§ 1030(c)(4)(E)) or if it is a second or subsequent offense (18 U.S.C. §§ 1030(c)(4)(C)) not more than twenty years and a fine of not more than $250,000 (18 U.S.C. § 3571(b)(3)) and if the offender attempts to cause or knowingly or recklessly causes death any term of years or life and a fine of not more than $250,000 (18 U.S.C. §§ 1030(c)(4)(F), 3571(b)(3)). Violations of the second offense are punishable by imprisonment of not more than one year and a fine of not more than $100,000 (18 U.S.C. §§ 1030(c)(4)(G), 3559(a)(6), 3571(b)(5)) and not more than twenty years and a fine of not more than $250,000 for second and subsequent offenses (18 U.S.C. §§ 1030(c)(4)(C), 3571(b)(3)). Violations of the third offense carry the same punishment except that the term of imprisonment of second and subsequent offenses may not exceed ten (rather than twenty) years (18 U.S.C. § 1030(c)(4)(D)).

[2489] Not that physical access tokens are not covered by this provision.

[2490] 18 U.S.C. § 1030(a)(6).

[2491] 18 U.S.C. §§ 1030(c)(2)(A), 3559(a)(6), 3571(b)(5).

[2492] *See* 18 U.S.C. §§ 1030(c)(2)(C), 3571(b)(3).

obtained from a protected computer without (sufficient) authorization; or (C) a demand or request for anything of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.[2493] Such a cyber extortion is punishable by imprisonment for not more than five years[2494] (not more than ten years for second and subsequent offenses)[2495] and a fine of not more than $250,000.[2496]

7.1.2. The Wiretap Act

The Wiretap Act[2497] establishes a number of criminal offenses with regard to the interception and disclosure of wire, oral, or electronic communications, the most significant of which is codified at 18 U.S.C. § 2511(1)(a)[2498]: Any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or

[2493] 18 U.S.C. § 1030(a)(7).

[2494] 18 U.S.C. § 1030(c)(3)(A).

[2495] 18 U.S.C. § 1030(c)(3)(B).

[2496] 18 U.S.C. § 3571(b)(3).

[2497] Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522 (2010)).

[2498] Other offenses include the intentional uses of a device to intercept oral communication (18 U.S.C. § 2511(1)(b)); the intentional disclosure of the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through an interception in violation of § 2511(1) (18 U.S.C. § 2511(1)(c)); the intentional use of the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through an interception in violation of § 2511(1) (18 U.S.C. § 2511(1)(d)); and the intentional disclosure of the contents of any wire, oral, or electronic communication, lawfully intercepted pursuant to the Wiretap Act with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation (18 U.S.C. § 2511(1)(e)). As regards, information security, these offenses are only of minor significance when compared to § 2511(1)(a): Subsection (1)(b) only applies to oral communication, (1)(c) only to the subsequent disclosure of information after an illegal interception, (1)(d) only to the "use" of intercepted information (which generally is not an information security issue; *see supra* chapter 2.2.1), and (1)(e) only to the disclosure of information performed with the intent to interfere with a criminal investigation.

electronic communication"[2499] shall be fined in the amount of not more than $250,000 or imprisoned for not more than five years, or both.[2500]

The statute defines "intercept" as "the aural or other *acquisition of the contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[2501] This makes clear that for an offense under § 2511(1)(a) to be committed, the "contents" of a communication has to be intercepted which "includes any information concerning the substance, purport, or meaning of that communication"[2502] but not information about "the existence of the communication or transactional records about it."[2503]

Electronic communications are defined broadly as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[2504] One court has construed this definition so as to exclude the transmission of keystrokes from a keyboard to the computer's CPU.[2505]

[2499] 18 U.S.C. § 2511(1)(a).

[2500] 18 U.S.C. §§ 2511(4)(a), 3571(b)(3).

[2501] 18 U.S.C. § 2510(4) (emphasis added). *Cf.* 18 U.S.C. § 2510(5) (defining "electronic, mechanical, or other device").

[2502] 18 U.S.C. § 2510(8).

[2503] S. REP. NO. 99-541, at 13 (1986). This creates significant uncertainties, in particular as to whether URLs are to be considered part of the "contents" of a web communication (a URL often contains user-supplied text such as a search term; e.g. http://google.com/search?q=wiretapping). *See* U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 59 (2007), *available at* http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf (noting that "[s]ome types of information concerning network communications, such as full-path URLs, may raise arguments about whether they contain content"). *Cf. also* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 51, 69 (2004) (criticizing the ambiguity created by the statute with regard to "web traffic data").

[2504] 18 U.S.C. § 2510(12).

[2505] United States v. Ropp, 347 F. Supp. 2d 831, 837 (C.D. Cal. 2004) (holding that using a hardware key logger to capture keystrokes of a user composing an e-mail does not constitute an interception of "electronic communication"). *But cf.* U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 60 (2007), *available at*

7.1.3. The Stored Communications Act

The Stored Communications Act[2506] which was enacted as Title II of the Electronic Communications Privacy Act of 1986[2507] provides punishment for anyone who intentionally accesses without (sufficient) authorization a facility through which an "electronic communication service"[2508] is provided and thereby "obtains," "alters," or "prevents authorized access to"[2509] a wire or electronic communication while it is in electronic storage in such system.[2510]

The statute defines "electronic storage" as (A) "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission" and (B) "any storage

http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf ("Notwithstanding the *Ropp* decision, prosecutors should pursue cases involving interceptions occurring on computers or internal networks that affect interstate commerce. For example, if an individual installs malicious software on the victim's computer that makes a surreptitious copy every time an email is sent, or captures such messages as they move on the local area network on their way to their ultimate destination half way around the world, such cases can be prosecuted under section 2511.").

[2506] Pub. L. No. 99-508, Title II, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701-11 (2010)).

[2507] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[2508] 18 U.S.C. § 2510(15) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications"). For example, providing e-mail accounts over the internet constitutes such a service. F.T.C. v. Netscape Communications Corp., 196 F.R.D. 559, 560 (N.D. Cal. 2000). However, a home computer typically does not provide any such services. *See* United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003). *But see* In re Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1277 (C.D. Cal. 2001) (allegation that website operator accessed data contained in "cookies" that it placed in users' computers' electronic storage was sufficient to state claim for violation of 18 U.S.C. § 2701). Businesses offering their traditional products and services online through a website are not providing an "electronic communication service." Dyer v. Nw. Airlines Corporations, 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004). *See also* Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (holding that the online merchant Amazon.com is not an electronic communication service provider). Note that the Stored Communications Act uses the term "electronic communication service" while other federal laws and EU Directives use the term "electronic communications service."

[2509] These three alternatives can also be described as a compromise of confidentiality, integrity, and availability.

[2510] 18 U.S.C. § 2701(a).

[…] for purposes of backup protection of such communication."[2511] This has been construed to exclude communication in post-transmission storage.[2512]

An offense is punishable by imprisonment for not more than one year and a fine of not more than $100,000. If it is the second offense under this provision[2513] or if the offense is committed for a specified improper purpose,[2514] it is punishable by imprisonment for not more than five years and a fine of not more than $250,000.[2515] For repeat violations committed for an improper purpose, the maximum penalty is imprisonment for a term of ten years and a fine of $250,000.[2516]

7.2. State Computer Crime Law

Since the meaning of a "protected computer" under CFAA has been interpreted very broadly,[2517] federal computer crime law has a very wide reach. CFAA generally does not preempt computer crime state laws;[2518] it does, however, reduce the practical importance of

[2511] 18 U.S.C. § 2510(17).

[2512] Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part, vacated in part, remanded*, 352 F.3d 107 (3d Cir. 2003) (holding that § 2510(17)(A) "covers a message that is stored in intermediate storage temporarily, after the message is sent by the sender, but before it is retrieved by the intended recipient" while § 2510(17)(B), by referring to "such communication" also does not cover "messages that are in post-transmission storage, after transmission is complete"). *Cf.* H.R. REP. NO. 647, at 65 (1986).

[2513] 18 U.S.C. § 2701(b)(2)(B).

[2514] 18 U.S.C. § 2701(b)(1) ("if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act […]").

[2515] 18 U.S.C. § 3571(b)(3).

[2516] 18 U.S.C. §§ 2701(b)(1)(B), 3571(b)(3).

[2517] *See supra* chapter 7.1.1.

[2518] *Cf.* Pac. Aerospace & Electronics, Inc. v. Taylor, 295 F. Supp. 2d 1188, 1194 (E.D. Wash. 2003) (noting with regard to CFAA as first passed in 1986 that "Congress was reluctant to preempt or interfere with the local and state computer crime authorities").

such state laws. Accordingly, the following chapters will only briefly outline California (see *infra* chapter 7.2.1) and New York (see *infra* chapter 7.2.2) computer crime statutes.

7.2.1. California State Law

Similar to CFAA, California Penal Code § 502(c) establishes a list of criminal offenses related to unauthorized access to computers or computer data: (1) knowingly accessing and without permission altering or otherwise using any data, computer system, or network to defraud or for the purpose of wrongfully controlling or obtaining money, property, or data;[2519] (2) knowingly accessing and without permission copying, or making use of any data from a computer system or network or taking or copying any supporting documentation;[2520] (3) knowingly and without permission using computer services;[2521] (4) knowingly accessing and without permission altering any data, computer software, or computer programs;[2522] (5) knowingly and without permission disrupting computer services or denying computer services to an authorized user;[2523] (6) knowingly and without permission providing a means of accessing a computer system or network in violation of § 502(c);[2524] (7) knowingly and

[2519] CAL. PENAL CODE § 502(c)(1) (West 2010).

[2520] CAL. PENAL CODE § 502(c)(2). *Cf. See* Facebook, Inc. v. ConnectU LLC, 489 F. Supp. 2d 1087, 1091 (N.D. Cal. 2007) (denying summary judgment in the defendant's favor because the defendant had copied data from Facebook's website in violation of Facebook's terms of use and therefore acted—despite having the consent of the individuals concerned—"without permission"). *But cf.* Facebook, Inc. v. Power Ventures, Inc., No. C 08-05780 JW, 2010 WL 3291750, at *8 (N.D. Cal. July 20, 2010) ("Contrary to the holding of *ConnectU*, the Court finds that allowing violations of terms of use to fall within the ambit of the statutory term 'without permission' does essentially place in private hands unbridled discretion to determine the scope of criminal liability").

[2521] CAL. PENAL CODE § 502(c)(3).

[2522] CAL. PENAL CODE § 502(c)(4). Whether the use of a Trojan horse that is, by definition, installed voluntarily by the victim, fulfills the "without permission" requirement is questionable. *See In re* Apple & ATTM Antitrust Litig., No. C 07-05152 JW, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010) (holding that "[v]oluntary installation runs counter to [§ 502(c)(4)'s] requirement that the act was "without permission").

[2523] CAL. PENAL CODE § 502(c)(5).

[2524] CAL. PENAL CODE § 502(c)(6).

without permission accessing any computer system or network;[2525] (8) knowingly introducing any computer contaminant (e.g. a virus)[2526] into any computer system or network;[2527] (9) knowingly and without permission using the Internet domain name of another to send e-mails that cause damage to a computer system or network.[2528]

In similarity to the Wiretap Act, California Penal Code § 632 prohibits the eavesdropping on or recording of "confidential communications."[2529]

7.2.2. New York State Law

New York state law also establishes a number of offenses related to the unauthorized use of computers: New York Penal Law § 156.05 makes it a class A misdemeanor to knowingly use

[2525] CAL. PENAL CODE § 502(c)(7).

[2526] CAL. PENAL CODE § 502(b)(12) (defining "[c]omputer contaminant" as "any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information [including] viruses or worms […]").

[2527] CAL. PENAL CODE § 502(c)(8).

[2528] CAL. PENAL CODE § 502(c)(9). Sanctions for violations of the offenses established by § 502(c) range from prison terms of not more than one year to not more than three years and/or a fine of not more than $1,000 to not more than $10,000. CAL. PENAL CODE § 502(d).

[2529] CAL. PENAL CODE § 632(a) ("Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication […] shall be punished […]"). Violations are punishable by imprisonment of not more than one year and a fine of not more than $2,500 ($10,000 for repeated offenders). *Id. See also* CAL. PENAL CODE § 632(c) (stating that "confidential communication" includes "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in [any] circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded"). Also note that CAL. PENAL CODE § 632 may, to some extent be preempted by the Wiretap Act. *See* 18 U.S.C. § 2518(10(c) ("The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications."). *See also* Bunnell v. Motion Picture Ass'n of Am., 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (holding that the federal ECPA preempts a claim under the more narrowly worded CAL. PENAL CODE § 623).

or "access"[2530] a computer, computer service,[2531] or computer network "without authorization."[2532]

Section 156.10 establishes computer trespass as a class E felony by prohibiting anyone from knowingly using or accessing a computer, computer service, or computer network without authorization if he either acts with intent to commit any felony or thereby knowingly gains access to "computer material."[2533]

Section 156.20 establishes the class A misdemeanor of computer tampering by prohibiting anyone from using or accessing a computer, computer service, or computer network without

[2530] N.Y. PENAL LAW § 156.00(7) (McKinney 2010) (defining "access" broadly as "to instruct, communicate with, store data in, retrieve from, or otherwise make use of any resources of a computer, physically, directly or by electronic means").

[2531] N.Y. PENAL LAW § 156.00(4) (defining "computer service" broadly as "any and all services provided by or through the facilities of any computer communication system allowing the input, output, examination, or transfer, of computer data or computer programs from one computer to another").

[2532] N.Y. PENAL LAW § 156.00(8) (defining "without authorization" as "[…] without the permission of the owner or lessor or someone licensed or privileged by the owner or lessor where such person knew that his or her use or access was without permission or after actual notice to such person that such use or access was without permission. It shall also mean the access of a computer service by a person without permission where such person knew that such access was without permission or after actual notice to such person, that such access was without permission.") Proof that the offender knowingly circumvented a security measure is considered presumptive evidence that he acted without authorization. *Id.* However, it is a valid defense "that the defendant had reasonable grounds to believe that he had authorization to use the computer." N.Y. PENAL LAW § 156.50(1). *Cf.* People v. Klapper, 902 N.Y.S.2d 305, 311 (N.Y. Crim. Ct. 2010) (stating that "the Legislative intent was to criminalize computer intrusions where the owner of the computer or service had sufficiently set forth protections or policies to avoid unauthorized access").

[2533] N.Y. PENAL LAW § 156.00(5) (defining "computer material" as "any computer data or computer program which: (a) contains records of the medical history or medical treatment of an identified or readily identifiable individual or individuals […]; or (b) contains records maintained by the state […] concerning a person […] which […] can be used to identify the person and which is otherwise prohibited by law from being disclosed; or (c) is not and is not intended to be available to anyone other than the person or persons rightfully in possession thereof or selected persons having access thereto with his, her or their consent and which accords or may accord such rightful possessors an advantage over competitors or other persons […]"). In re Shubov, 802 N.Y.S.2d 437, 440 (N.Y. App. Div. 2005) (a voice mail in a competitor's voice mail system constitutes "computer material").

authorization[2534] to intentionally alter computer data or a computer program of another person.[2535] Case law suggests that this may also cover certain denial of service attacks.[2536]

Section 156.29 makes it a class B misdemeanor to duplicate in any manner, without the right to do so, computer material that contains records of the medical history or medical treatment of an identified or readily identifiable individual with intent to commit any crime under New York Penal Law.

Section 156.30 makes it class E felony to duplicate in any manner, without the right to do so, any computer data[2537] or computer program, if the offender either thereby intentionally and wrongfully deprives or appropriates an economic value or benefit in excess of $2,500 or acts with intent to commit any felony.[2538]

Section 156.35 also makes it a class E felony to knowingly possess, without a right to do so, a duplicate of any computer data or computer program created in violation of § 156.30 with intent to benefit himself or a person other than an owner thereof.[2539]

[2534] *Cf.* N.Y. PENAL LAW § 156.50(2) (stating that "it shall be a defense that the defendant had reasonable grounds to believe that he had the right to alter in any manner or destroy the computer data or the computer program").

[2535] In addition to this class A misdemeanor, N.Y. PENAL LAW §§ 156.25, 156.26, and 156.27 establish the class E, D, and C felonies of computer tampering in the third, second, and first degree.

[2536] *See* People v. Versaggi, 629 N.E.2d 1034, 1039 (N.Y. 1994) (holding that the defendant "altered" computer programs when he activated existing instructions in his employer's computer system which commanded computers to shut down and interrupt telephone service to employer's offices). Under this holding, making a program crash, constitutes an "alteration" of that program.

[2537] *See* N.Y. PENAL LAW § 156.00(3) (defining "computer data" as any information that is "processed, or ha[s] been processed in a computer"). *Cf.* People v. Angeles, 687 N.Y.S.2d 884, 887 (N.Y. Crim. Ct. 1999) (a print-out of a customer list that could only be accessed and printed through a computer system constitutes computer data).

[2538] *Cf.* N.Y. PENAL LAW §§ 156.50(3) (stating that it "shall be a defense that the defendant had reasonable grounds to believe that he had the right to […] duplicate […] the computer data or the computer program").

[2539] *Cf.* People v. Katakam, 660 N.Y.S.2d 334, 336 (N.Y. Sup. Ct. 1997) (any intention by defendant to sell former employer's proprietary computer script files, to use them in his new position in order to advance himself

Lastly, New York Penal Law § 250.05 makes it a class E felony to unlawfully[2540] engage in wiretapping,[2541] mechanical overhearing of a conversation,[2542] or intercepting or accessing of an electronic communication.[2543]

7.3. EU Framework Decision on Attacks Against Information Systems

Council Framework Decision 2005/222[2544] (hereinafter *Framework Decision*) was introduced to address "[s]ignificant gaps and differences in Member States' laws"[2545] in the area of attacks against information systems. It introduces three distinct criminal offenses[2546] and also requires the criminalization of instigation, aiding and abetting, and attempt.[2547]

At this point it should be noted that the Framework Decision largely parallels the Council of Europe's Convention on Cybercrime[2548] which was signed by all and ratified by 17 Member

or to save himself labor, or to study and learn from them would satisfy the requirement that he intended to benefit himself).

[2540] This refers to a lack of a permissible eavesdropping by law enforcement officers under N.Y. CRIM. PROC. LAW art. 700.

[2541] Wiretapping only covers telephonic or telegraphic communication. N.Y. PENAL LAW § 250.00(1).

[2542] Mechanical overhearing only covers face-to-face communications. *See* N.Y. PENAL LAW § 250.00(2) (referring to "a person not present [at the conversation or discussion]").

[2543] *See* N.Y. PENAL LAW § 250.00(6) (defining "intercepting or accessing of an electronic communication" as "the intentional acquiring, receiving, collecting, overhearing, or recording of an electronic communication, without the consent of the sender or intended receiver thereof, by means of any instrument, device or equipment, except when used by a telephone company in the ordinary course of its business or when necessary to protect the rights or property of such company"); *id.* § 250.00(5) (defining "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system […]").

[2544] 2005 O.J. (L 69) 67 (JHA).

[2545] Framework Decision recital 5.

[2546] Framework Decision art. 2-4.

[2547] Framework Decision art. 5. The only offense the attempt of which does not have to be prohibited is illegal access to information systems (art. 2). *See* Framework Decision art. 5(3).

[2548] Convention on Cybercrime, Nov. 23, 2001, Council of Europe CETS No. 185, 2296 U.N.T.S. 167. Note that the Convention on Cybercrime additionally contains the offenses of illegal interception (Convention on

States.[2549] However, since the Convention on Cybercrime is not a legislative act of the EU but an international treaty, it is outside the scope of this thesis.[2550]

Framework Decision article 2 requires Member States to establish, as a criminal offense, the intentional access "without right"[2551] to the whole or any part of an "information system,"[2552] at least for cases which are not "minor"[2553] and where the offense is committed by infringing a security measure.[2554]

Since the Framework Decision does not define what is to be understood under "minor" cases,[2555] some Member States have construed this exception liberally, limiting offenses under article 2 to (1) cases where the offender has the intent to perpetrate data espionage, use

Cybercrime art. 3) and possession or making available of hacker tools and passwords (Convention on Cybercrime art. 6).

[2549] The following Member States have not ratified the Convention on Cybercrime: Austria, Belgium, Czech Republic, Greece, Ireland, Luxembourg, Malta, Poland, Sweden, and the United Kingdom. *See* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=29/11/2010&CL=ENG (last accessed Feb. 10, 2011).

[2550] For a discussion of the added value of the Framework Decision over the Convention on Cybercrime, in particular regarding jurisdictional conflicts see Paul De Hert et al., *Fighting Cybercrime in the Two Europes: The Added Value of the EU Framework Decision and the Council of Europe Convention*, 77 INT'L REV. OF PENAL L. 503, 523 (2006).

[2551] Framework Decision art. 1(d) (defining "without right" as "not authorized by the owner, other right holder of the system or part of it, or not permitted under the national legislation").

[2552] The term "information system" is defined broadly as "any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance." Framework Decision art. 1(a).

[2553] Framework Decision art. 2(1).

[2554] *Id*. Note that at least one Member State has initially interpreted "infringing" as "damaging" a security measure. *See* LUKAS FEILER, ZUR STRAFRECHTLICHEN BEURTEILUNG VON IT-SICHERHEITSLÜCKEN [ON THE EVALUATION OF IT SECURITY VULNERABILITIES IN CRIMINAL LAW] 30, 36 (2006), http://lukasfeiler.com/Zur_strafrechtlichen_Beurteilung_von_IT-Sicherheitsluecken.pdf (discussing why "hacking" was not an offense under Austrian criminal law unless a security measure had been damaged ("verletzt") and describing why the exploitation of code injection, SQL injection, and race condition vulnerabilities does not damage any security measures; with reference to the specific technical vulnerabilities discussed in this paper, the law was amended in 2007; *see* Nationalrat [NR] [National Council] Gesetzgebungsperiode 23 Beilage [Blg] No. 285, at 7 (Austria).

[2555] It only states that "[t]here is a need to avoid over-criminalisation, particularly of minor cases, as well as a need to avoid criminalizing right-holders and authorised persons." Framework Decision recital 13.

the data obtained in order to make a profit or to cause damage;[2556] (2) cases where the data is subsequently misused or damaged;[2557] (3) cases where the data accessed is "endangered";[2558] or (3) cases where substantial injury is caused.[2559] The Commission has expressed "serious reservations" regarding the permissibility of such limitations.[2560]

Article 3 of the Framework Decision requires Member States to outlaw the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data when committed without right, at least for cases which are not minor.

Similarly, Framework Decision article 4 requires Member States to prohibit the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system when committed without right, at least for cases which are not minor.

Offenses under articles 3 and 4 have to be punishable by criminal penalties of a maximum of at least between one and three years of imprisonment.[2561] Offenses under article 2 as well as

[2556] *See* Strafgesetzbuch [StGB] [Criminal Code], BGBl. No. 60/1974, as amended, § 118a(1) (Austria). *Cf.* Lukas Feiler, *Neue Bedrohungen aus dem Internet – Botnets: Spamming, Phishing und DDoS Attacks im großen Stil* [*New Internet Threats—Botnets: Spamming, Phishing, and DDoS Attacks on a Large Scale*], ANWALT AKTUELL, Mar. 2007, at 30. *Cf. also Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*, at 4, COM (2008) 448 final (July 14, 2008).

[2557] This is the case in the Czech Republic. *See id.*

[2558] This is the case in Finland. *See id.*

[2559] This is the case in Latvia. *See id.*

[2560] *See id.* (therefore concluding that at least four Member States have not properly implemented article 2 of the Framework Decision). Note, however, that the Commission seems to indicate that accessing a computer without compromising the confidentiality of data would constitute a "minor" case. *Id.* at 4 (stating that "the concept of 'minor case' must refer to cases where instances of illegal access are of minor importance or where an *infringement of information system confidentiality* is of a minor degree" (emphasis added)).

[2561] Framework Decision art. 6(2).

any instigation, aiding and abetting, or attempt only have to be punishable by "effective, proportional and dissuasive criminal penalties."[2562] When committed within the framework of a "criminal organization,"[2563] offenses under articles 3 and 4 as well as article 2 if committed by infringing a security measure have to be punishable by criminal penalties of a maximum of at least between two and five years of imprisonment.[2564]

Aside from substantive criminal law, the Framework Decision provides rules on jurisdiction[2565] and on the liability of legal persons: They can be held liable for offenses committed for their benefit by any person who has a leading position within the legal person[2566] as well as for offenses made possible by the lack of supervision or control by such a person if committed for their benefit by a person under their authority.[2567]

Lastly it should be noted that the European Commission has proposed a directive to replace the Framework Decision.[2568] This directive would retain most of the Framework Decision's

[2562] Framework Decision art. 6(1).

[2563] *See* Joint Action 98/733, art. 1, 1998 O.J. (L 351) 1, 1 (JHA) (defining "criminal organization" as "a structured association, established over a period of time, of more than two persons, acting in concert with a view to committing offences which are punishable by deprivation of liberty or a detention order of a maximum of at least four years or a more serious penalty, whether such offences are an end in themselves or a means of obtaining material benefits and, where appropriate, of improperly influencing the operation of public authorities").

[2564] Framework Decision art. 7(1). *Cf. Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*, at 8, COM (2008) 448 final (July 14, 2008) (noting that at least four Member States do not comply with art. 7).

[2565] *See* Framework Decision art. 10.

[2566] Framework Decision art. 8(1). A "leading position" must be based on "(a) a power of representation of the legal person, or (b) an authority to take decisions on behalf of the legal person, or (c) an authority to exercise control within the legal person." *Id.*

[2567] Framework Decision art. 8(2).

[2568] *Commission Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, COM (2010) 517 final (Sept. 30, 2010).

provisions but would add the offenses of (1) illegal interception[2569] and (2) producing, selling, procuring for use, importing, distributing or otherwise making available tools used for committing any of the other offenses.[2570]

7.4. Comparative Assessment

7.4.1. The Attribution Problem—An Inherent Limitation of Deterrence

Criminal law can deter malicious threat agents from mounting any threats in two ways: (1) when an offender is punished for a criminal act, he may be deterred from committing such a crime in the future (*specific deterrence*) and (2) when potential future offenders learn of the threatened punishment, they may decide not to commit the crime (*general deterrence*).[2571]

It is well recognized that the extent to which criminal law can act as a deterrent largely depends on the *certainty of punishment* as opposed to its severity.[2572] In other words, the probability that malicious threat agents will be prosecuted, should they violate a criminal law, largely determines the deterrent effect of the criminal law, irrespective of the severity of

[2569] *See id.* at 14 (proposing the criminalization of "the intentional interception by technical means, of non-public transmissions of computer data to, from or within a information system, including electromagnetic emissions from an information system carrying such computer data, is punishable as a criminal offence when committed without right").

[2570] This prohibition would apply to "device, including a computer program, designed or adapted primarily for the purpose of committing any of the [other] offences" and "a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed." *Id.* at 14.

[2571] *Cf., e.g.,* STEPHEN E. BROWN ET AL., CRIMINOLOGY: EXPLAINING CRIME AND ITS CONTEXT 182 (7th ed. 2010).

[2572] *See* Jerry Parker & Harold G. Grasmick, *Linking Actual and Perceived Certainty of Punishment: An Exploratory Study of an Untested Proposition in Deterrence Theory*, 17 CRIMINOLOGY 366 (1979); Raymond Paternoster, *Assessments of Risk and Behavioral Experience: An Exploratory Study of Change*, 23 CRIMINOLOGY 417 (1985); Julie Horney & Ineke Marshall, *Risk Perceptions Among Serious Offenders: The Role of Crime and Punishment*, 30 CRIMINOLOGY 575 (1992). *Cf. also* CESARE BECCARIA, AN ESSAY ON CRIMES AND PUNISHMENTS 62 (Adolph Caso trans., 2008) (1764) ("The certainty of a small punishment will make a stronger impression, than the fear of one more severe, if attended with the hopes of escaping"); LAW REFORM COMM'N OF CANADA, FEAR OF PUNISHMENT: DETERRENCE 28 et seq. (1976) (providing further references).

potential punishment. Empirical studies demonstrate that this also applies to computer crime laws.[2573]

A precondition for prosecution—and therefore for a criminal law's deterrent effect—is that an attack can be attributed to the actual offender. However, the Internet—the architecture over which most attacks on the security of information and information systems are carried out—does not provide any built-in identification, let alone authentication mechanisms.[2574] The architecture of the Internet only provides for the ability to trace the IP address that was used to perform a given attack to a particular Internet access provider[2575] which may or may not have further records about the organization or individual to whose Internet access account the IP address was assigned at the time in question. Even if an Internet access provider maintains such information, it will only identify the holder of the Internet access account but not the individual who actually used the Internet access to perform the attack. Since a single Internet access account is often shared by all members of a household at least and potentially hundreds of people in a corporate setting, this type of "identification" is often insufficient for purposes of a criminal prosecution.

[2573] *See* I.P.L. PNG & CHEN-YU WANG, THE DETERRENT EFFECT OF ENFORCEMENT AGAINST COMPUTER HACKERS: CROSS-COUNTRY EVIDENCE 11 (SIXTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, WORKING PAPER, 2007), *available at* http://weis2007.econinfosec.org/papers/77.pdf (finding that government enforcement reduces attacks against computer networks by an average of 36% during a 15-day window).

[2574] Famously summarized by the caption of a Peter Steiner cartoon published in THE NEW YORKER, July 5, 1993, at 61: "On the Internet, nobody knows you're a dog." *Cf. also* LAWRENCE LESSIG, CODE: VERSION 2.0, at 35 (2006).

[2575] *See supra* chapter 2.3.1 (discussing the assignment of IP address ranges to Autonomous Systems on the Internet).

More importantly, whatever the status of sophistication of the identification and authentication mechanisms is today or may be in the future,[2576] most malicious threat agents will find a way to circumvent them. Once an attacker compromises a single personal computer of another Internet user, that computer can be used to perform other attacks that will appear to originate from the innocent Internet user's PC. By tunneling his activities through multiple compromised computers, possibly located in different jurisdictions, an attacker can make it virtually impossible for investigators to learn his identify.[2577]

The "attribution problem" is therefore an inherent aspect of computer crime unlikely to be sufficiently addressed by any technological solution. Accordingly, the *certainty of punishment* for computer crimes will continue to be very low for the foreseeable future. Since the deterrent effect of criminal law largely depends on the *certainty of punishment*,[2578] computer crime law is an inherently poor deterrent for malicious threat agents.[2579]

[2576] *Cf.* Richard L. Kugler, *Deterrence of Cyber Attacks, in* CYBERPOWER AND NATIONAL SECURITY 309, 337 (Franklin D. Kramer et al. eds., 2009) (suggesting that the "attribution problem" could be addressed by "better technical attribution capabilities so that the sources of all attacks can be identified," thereby implicitly assuming that such technical capabilities would be impossible to circumvent).

[2577] *Cf.* DONN B. PARKER, FIGHTING COMPUTER CRIME: A NEW FRAMEWORK FOR PROTECTING INFORMATION 177 (1998) ("Computer viruses […] are generally written and distributed by hackers (by definition). But, because these hackers are difficult to identify in the huge, anonymous maze of cyberspace, they are rarely apprehended or prosecuted."); Clay Wilson, *Cyber Crime, in* CYBERPOWER AND NATIONAL SECURITY 415, 416 (Franklin D. Kramer et al. eds., 2009) (noting that "[t]he possibility of illicit profits, together with a low probability of detection or identification, can make cyber crime attractive"). *Cf. also* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 75 et seq. (2008) (arguing that the ease with which cybercrimes can be perpetrated while hiding one's identity result in a situation where only the stupid are caught).

[2578] *See supra*.

[2579] Furthermore, it needs to be recognized that computer crime law—as all deterrent measures—only mitigates threats originating from *malicious* threat agents. Risks originating from non-malicious threat agents, such as humans making mistakes or the force of nature, are not at all reduced by computer crime law.

7.4.2. The Application to Botnets as a Touchstone for Computer Crime Law

To the extent that computer crime law can serve as a deterrent despite a low *certainty of punishment*,[2580] it is critical that the law actually covers the most significant threats to the security of information and information systems.

One threat that is of particular significance in today's information security landscape is that of *botnets*.[2581] The term botnet refers to a virtual network of compromised computers ("zombies"). A piece of remote control software (referred to as a "bot") runs on every compromised computer, thereby giving the attacker (referred to as the "bot herder") full control over the entire botnet as well as every computer individually. In the past, botnets have been discovered that consisted of millions of computers.[2582] According to an estimate by *Vint Cerf*, up to a quarter of the computers connected to the Internet may, at any time, be part of a botnet.[2583]

How well computer crime laws apply to the threat of botnets serves as an excellent indicator for the general effectiveness of these laws. It will therefore be analyzed *infra* to what extent

[2580] *See supra* chapter 7.4.1.

[2581] *Cf. Commission Staff Working Document, Impact Assessment, Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems, and repealing Council Framework Decision 2005/222/JHA*, at 8, SEC (2010) 1122 final (Sept. 9, 2010) ("A number of ways to carry out an attack have been observed. However, most important and threatening are botnets […]").

[2582] For example, the Conficker botnet is estimated to have consisted of eight to 15 million computers. *Cf.* John Markoff, *Worm Infects Millions of Computers Worldwide*, N.Y. TIMES, Jan. 22, 2009, at A12, *available at* http://www.nytimes.com/2009/01/23/technology/internet/23worm.html; United Press Int'l, *Virus strikes 15 million PCs*, UPI.COM, Jan. 26, 2009, http://www.upi.com/Top_News/2009/01/26/Virus-strikes-15-million-PCs/UPI-19421232924206/.

[2583] *See* Tim Weber, *Criminals 'may overwhelm the web,'* BBC NEWS, Jan. 25, 2007, http://news.bbc.co.uk/1/hi/business/6298641.stm. *Cf.* Press Release, Eurostat, European Comm'n, Nearly one third of internet users in the EU27 caught a computer virus (Feb. 7, 2011), *available at* http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-07022011-AP/EN/4-07022011-AP-EN.PDF (finding that 31% who used the Internet in the 12 months prior to the survey reported that they caught a virus or other computer infection resulting in loss of information or time during this period).

the computer crime laws discussed above criminalize compromising computers for the purpose of integrating them into a botnet. This analysis will focus on botnets as general-purpose tools and will not specifically address the uses to which botnets can be put.

In many cases, computers are compromised and joined into a botnet not because the attacker is interested in the information they store but rather because the attacker wants to make use of the computer power and bandwidth of the computers. For example, many botnets are (only) used to send unsolicited e-mails[2584] or perform distributed denial of service (DDoS) attacks on third parties.[2585] In other cases, the purpose of the botnet remains unknown until it has grown to a sufficiently large size.[2586] This raises the question of whether compromising a computer constitutes a crime even if the attacker does not (and has no provable intent to) alter, obtain, or delete any information stored on the computer.

Under CFAA, accessing a computer without (sufficient) authorization does not constitute a crime unless information is obtained (18 U.S.C. § 1030(a)(2)), it is a nonpublic federal government computer (§ 1030(a)(3)), the attacker acts with an intent to defraud (§ 1030(a)(4)), or damage is caused (§ 1030(a)(5)). Accordingly, the creation of a botnet for the purpose of sending spam only constitutes a crime under CFAA if the installation of the

[2584] *See* CRAIG A. SCHILLER ET AL., BOTNETS: THE KILLER WEB APP 51 (2007). Albeit not an information security issue, it should be noted that sending spam does not necessarily constitute a criminal offense under U.S. federal law or the law of EU Member States. *See* 18 U.S.C. § 1037(a)(3); Parliament and Council Directive 2000/31, art. 7, 2000 O.J. (L 178) 1, 11.

[2585] *See* CRAIG A. SCHILLER ET AL., BOTNETS: THE KILLER WEB APP 46 (2007).

[2586] For example, the botnet "Conficker" which was first detected in November 2008 was not used at all by its bot herder(s) until April 2009. *See* Gregg Keizer, *Conficker cashes in, installs spam bots and scareware*, COMPUTERWORLD, Apr. 9, 2009, http://www.computerworld.com/s/article/9131380/Conficker_cashes_in_installs_spam_bots_and_scareware?taxonomyName=Security.

bots on the compromised computers is considered "damage."[2587] This is, however, debatable.[2588]

Under California Penal Code § 502(c)(7) and New York Penal Law § 156.05, such conduct clearly constitutes a criminal offense since both provisions do not require the causation of any damages.[2589]

Article 2 of the EU Framework Decision in principal covers all unauthorized access irrespective of the purpose for which the access is (mis)used once obtained. However, it does not cover "minor" cases. This has been interpreted by some Member States as limiting article 2 to cases where the offender accessed the computer for the purpose of obtaining or damaging information.[2590] Such construction would render the Framework Decision inapplicable to many botnets.[2591]

Compromising computers for the sole purpose of joining them into a botnet is therefore only clearly covered by the California Penal Code and New York Penal Law but not under U.S. federal law or EU law.

[2587] *Cf. supra* chapter 7.1.1.

[2588] No case law exists on this point. It could be argued that the installation of the bot software constitutes an "impairment to the integrity [of] a system" (*see* 18 U.S.C. § 1030(e)(8) (defining "damage")). This is certainly the case, if the bot modifies the operating system in order to hide itself from anti-malware software, in which case the bot would be referred as a *rootkit*. *Cf. supra* chapter 3.1 (briefly introducing rootkits). However, this is less clear if the bot does not actually alter any existing data or software but only installs itself (thereby only using previously unused portions of the hard drive).

[2589] *See supra* chapters 7.2.1 and 7.2.2.

[2590] *See supra* chapter 7.3.

[2591] Note that the newly proposed Directive should eliminate this shortcoming. While it would retain the possibility to exempt "minor" cases, "[t]his possibility […] should not however lead to the introduction of additional constitutive elements of offences beyond those that are already included in the Directive, [e.g.] the presence of a specific effect such as causing a considerable damage." *Commission Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, at 7-8, COM (2010) 517 final (Sept. 30, 2010).

Another important question is whether these computer crime laws cover all possible ways of gaining unauthorized access to a computer. Generally, there are two ways of remotely compromising a computer: (1) by exploiting software vulnerabilities and (2) by means of social engineering.[2592] While the former is clearly within the scope of the computer crime laws discussed above, the latter raises questions with regard to the "unauthorized" nature of the access as well as with regard to the infringement of a security measure.

Social engineering describes the practice of manipulating people in an attempt to make them disclose confidential information or perform other actions that compromise information security.[2593] This does not only cover manipulations performed by an attacker in person but most significantly also includes the use of "Trojan horses." These are programs that appear benign but actually contain hidden malicious functionality.[2594] Since users are deceived about that functionality, they "voluntarily" install them on their computers.

A federal district court in California has recently held that a voluntary installation of software that contains hidden functionality does not constitute access "without authorization" for the purposes of 18 U.S.C. § 1030(a)(5) or "without permission" for the purposes of California

[2592] A third but not equally relevant possibility would be to compromise the source code repository of a popular software and to integrate a back door into the software. *Cf.* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 738 (3d ed. 2003) (describing how a back door was inserted into the OpenSSH software distributed by the OpenBSD Project); Dan Goodin, *Hackers poison well of open-source FTP app: ProFTPD backdoored for 3 days*, THE REGISTER, Dec. 2, 2010, http://www.theregister.co.uk/2010/12/02/proftpd_backdoored/; SourceForge, Sourceforge.net attack (Jan. 27, 2011), http://sourceforge.net/blog/sourceforge-net-attack/ (announcing that the source code of more than 230,000 open source software projects hosted on SourceForge's servers might have been compromised).

[2593] *See supra* chapter 2.4.2.

[2594] *See* NIST, GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING, SPECIAL PUBLICATION 800-83, at 2-4 (2005), *available at* http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf. This type of malware is named after the wooden horse from Greek mythology. Unfortunately, the term Trojan—which, if we continued the analogy, would refer to the victim of a Trojan horse attack—is often used synonymous with Trojan horse.

Penal Code § 502(c)(4).[2595] This holding raises serious doubt whether Trojan horse attacks are generally covered by CFAA and California Penal Code § 502(c).

The second question is whether social engineering involves "infringing a security measure." This is highly significant under article 2 of the Framework Decision which allows Member States to limit the criminalization of illegal access to computer systems to cases where the offense is committed "by infringing a security measure."[2596] This question can only be answered in the affirmative if the good judgment of people is considered a "security measure."[2597] However, some Member States have transposed article 2 of the Framework Decision by limiting offenses to cases where a "security measure *within the information system*" is infringed,[2598] thereby effectively excluding social engineering attacks.[2599]

In summary, reviewing the hacking of computers for the sole purpose of joining them in a botnet reveals legal uncertainties under CFAA as well as under the Framework Decision. Even more significant uncertainties exist regarding the question of whether social engineering (e.g. by using Trojan horses) falls within the scope of CFAA, California Penal Code § 502(c),

[2595] *In re* Apple & ATTM Antitrust Litig., No. C 07-05152 JW, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010) (holding with regard to the allegation that Apple violated CFAA and the California Penal Code by providing a software update that, when (voluntarily) installed, rendered some of its customers' phones unusable: "Voluntary installation runs counter to […] CFAA's requirement that the alleged act was 'without authorization' as well as the CPC's requirement that the act was 'without permission.' 18 U.S.C. § 1030(a)(5)(A)(I); [CAL. PENAL CODE] § 502(c)(4).").

[2596] *See* Framework Decision art. 2(2).

[2597] From an information security perspective, people should certainly be considered part of the security system. *Cf.* ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 17 et seq. (2d ed. 2008).

[2598] *See, e.g.,* Strafgesetzbuch [StGB] [Criminal Code], BGBl. No. 60/1974, as amended, § 118a(1) (Austria).

[2599] *Cf.* LUKAS FEILER, ZUR STRAFRECHTLICHEN BEURTEILUNG VON IT-SICHERHEITSLÜCKEN [ON THE EVALUATION OF IT SECURITY VULNERABILITIES IN CRIMINAL LAW] 44 (2006), http://lukasfeiler.com/Zur_strafrechtlichen_Beurteilung_von_IT-Sicherheitsluecken.pdf.

or Framework Decision article 2. With regard to New York Penal Law § 156.05, no court has yet addressed the issue.

8. Concluding Comparative Assessment

This chapter presents a concluding comparative assessment of information security law in the EU and the U.S. This assessment serves a twofold purpose: First, it is intended to provide an overview of the current state of regulation. Second, it aims to highlight general deficiencies of the current regulatory approaches of EU and U.S. regulatory policy. These deficiencies will serve as the basis for the policy recommendations made *infra* in chapter 9.

The concluding assessment will first consider the utilization of risk treatment options (see *infra* chapter 8.1) and will examine which actors of the information security landscape were in the focus of regulatory efforts (see *infra* chapter 8.2). Lastly, it will assess to what extent EU and U.S. law currently meet the fundamental challenges of information security (see *infra* chapter 8.3).

8.1. Utilization of Risk Treatment Options

As explained *supra* in chapter 3.2, any policy that explicitly addresses information security risks can do so by implementing one of the following risk treatment options: risk avoidance, risk mitigation, or risk transfer.[2600] The analysis of current EU and U.S. law in chapters 4 to 7 shows an uneven picture:

Complete risk avoidance is never explicitly considered as an appropriate policy option. Indeed, no policy currently implemented in EU or U.S. law aims to avoid all risks associated with a particular information asset by mandating the elimination of the asset itself. It is rather

[2600] *Cf. supra* chapter 3.2 (discussing these risk treatment options). Note that the risk treatment option of risk retention is not mentioned here since it does not address information security risks. Choosing risk retention rather means to do the opposite (accepting the risk as it is). *Cf. supra* chapter 3.2.4.

assumed that risk treatment measures will reduce risks to a level at which the benefits of keeping an information asset generally outweigh the associated risks.

Risk mitigation, in particular in its indirect form, is by far the most common policy option. Using a form of indirect risk mitigation, many regulatory policies require regulated entities to implement "reasonable" or certain specific security controls.[2601]

U.S. law establishes such security requirements for personal information controllers (see HIPAA Security Rule,[2602] GLBA § 501(b),[2603] FCRA,[2604] COPPA,[2605] Communications Act § 222,[2606] FTC Act § 5(a),[2607] and various California and New York state laws[2608]), publicly traded companies (see SOX §§ 302, 404[2609]), users, owners and operators of the bulk-power system (see NERC Standards[2610]), government authorities (see FISMA[2611]), as well as manufacturers of medical device software (see FFDCA § 520(f)[2612]). EU law establishes similar—although generally less stringent—security requirements for personal information

[2601] *Cf. supra* chapter 4.1.10.4 (discussing the advantages and disadvantages of "reasonable" and specific security requirements).

[2602] *See supra* chapter 4.1.1.

[2603] *See supra* chapter 4.1.2.

[2604] *See supra* chapter 4.1.3.

[2605] *See supra* chapter 4.1.4.

[2606] *See supra* chapter 4.1.5.

[2607] *See supra* chapter 4.1.6.

[2608] *See supra* chapter 4.1.7.

[2609] *See supra* chapter 4.2.1.

[2610] *See supra* chapter 4.3.2.

[2611] *See supra* chapter 4.4.1.

[2612] *See supra* chapter 4.5.1.

controllers (see EUDPD article 17,[2613] ePrivacy Directive article 4[2614]), certification-service-providers (see eSignature Directive annex II [2615]), providers of communications services (see Telecoms Framework Directive article 13a[2616]), manufacturers of medical device software (see Medical Devices Directive annex I[2617]), and manufacturers of certain signature products (see eSignature Directive annex III[2618]) but not for publicly traded companies[2619] or government authorities.[2620]

Another method by which policy makers attempt to mitigate risk is by mandating a notification of breaches of the security of personal information. Such measures are primarily intended to serve as a detective security control that allows individuals (and public authorities) to take appropriate reactive measures.[2621] While the EU has only adopted a single data security breach notification policy exclusively for the telecommunications sector (see ePrivacy Directive article 4(3)[2622]), U.S. federal law as well as state law implements a great number of breach notification regimes (see California Senate Bills 1386[2623] and 541,[2624] New

[2613] *See supra* chapter 4.1.8.

[2614] *See supra* chapter 4.1.9.

[2615] *See supra* chapter 4.3.3.

[2616] *See supra* chapter 4.3.1.

[2617] *See supra* chapter 4.5.2.

[2618] *See supra* chapter 4.5.3.

[2619] *See supra* chapter 4.2.2 (discussing the Fourth Company Law Directive).

[2620] *See supra* chapter 4.4.2 (discussing the internal security regulations of the Commission and the Council which only apply to classified information).

[2621] *Cf. supra* chapter 6.2.10.2 (providing a critical perspective on the choice of this risk treatment option).

[2622] *See supra* chapter 6.2.9.

[2623] *See supra* chapter 6.2.1.

[2624] *See supra* chapter 6.2.2.

York ISBNA,[2625] HITECH Act §§ 13402, 13407,[2626] GLBA § 501(b),[2627] Communications Act § 222,[2628] VA Breach Notification Rule,[2629] and OMB Memorandum M-07-16[2630]).

Similarly to data security breach notification, network security breach notification is also implemented by EU and U.S. law as a detective risk mitigation measure. The purpose of the FCC Network Outage Reporting Rule[2631] as well as Telecoms Framework Directive article 13a(3)[2632] is to keep public authorities informed so that they can make better risk decisions.[2633]

Implementing a form of direct risk mitigation, EU law as well as U.S. law further attempts to deter malicious threat agents by providing criminal sanctions for computer-related crimes. While there has been much legislative activity in this regard in the U.S. (see CFAA,[2634] Wiretap Act,[2635] Stored Communications Act,[2636] California Penal Code § 502,[2637] and New York Penal Law §§ 156.05-35, 250.05[2638]), the EU has only adopted a single legislative

[2625] *See supra* chapter 6.2.3.

[2626] *See supra* chapter 6.2.4.

[2627] *See supra* chapter 6.2.5.

[2628] *See supra* chapter 6.2.6.

[2629] *See supra* chapter 6.2.7.

[2630] *See supra* chapter 6.2.8.

[2631] *See supra* chapter 6.3.1.

[2632] *See supra* chapter 6.3.2.

[2633] *Cf. supra* chapter 6.3.3.1 (providing a critical perspective regarding the chosen risk treatment option).

[2634] *See supra* chapter 7.1.1.

[2635] *See supra* chapter 7.1.2.

[2636] *See supra* chapter 7.1.3.

[2637] *See supra* chapter 7.2.1.

[2638] *See supra* chapter 7.2.2.

measure, the Framework Decision on Attacks Against Information Systems.[2639] Both EU and U.S. computer crime law do not fully address common threats, in particular with regard to botnets,[2640] and suffer from an inherently low certainty of punishment.[2641]

Taken together, these preventive measures (in the form of mandatory security controls), detective measures (in the form of data and network security breach notification), and deterrent measures (in the form of computer crime law) signify a strong regulatory emphasis on risk mitigation measures.

Regulatory policies that implement the risk treatment option of a risk transfer do so either by assigning liability (which constitutes a direct risk transfer)[2642] or by mandatory disclosure of security-related information (which constitutes an indirect transfer).[2643]

The strongest form of liability assignment can be found in the areas of payment services and certification services: Both EU and U.S. law significantly limit the liability of payment service users, thereby reversing a risk transfer that would otherwise occur by contractual means (see Truth in Lending Act § 133(a),[2644] Electronic Fund Transfer Act § 909(a),[2645] and

[2639] *See supra* chapter 7.3.

[2640] *Cf. supra* chapter 7.4.2 (discussing the importance of botnets in the context of EU and U.S. computer crime law).

[2641] *See supra* chapter 7.4.1 (discussing the attribution problem as an inherent limitation to the effectiveness of computer crime law).

[2642] *Cf. supra* chapter 3.2.3.1.

[2643] *Cf. supra* chapter 3.2.3.2 (describing the nature of an indirect risk transfer and the basic principles of targeted transparency).

[2644] *See supra* chapter 5.4.1.

[2645] *See id*.

Payment Services Directive article 61[2646]). EU law also provides a rather strong liability regime for certification-service-providers (see eSignature Directive article 6[2647]).

However, outside these rather limited areas, EU and U.S. law do not perform any significant direct risk transfers. Under U.S. law, personal information controllers can generally not be held liable for the damages typically caused by security breaches, neither under federal statutory law (see HIPAA Safeguards Rule,[2648] GLBA,[2649] FCRA,[2650] COPPA[2651]), nor under state statutory law[2652] or common law.[2653] EU law is very vague as regards the liability of personal information controllers (see EUDPD article 23[2654]). Communications service providers and online service providers are largely shielded from liability under EU law (see E-Commerce Directive articles 12 to 14[2655]) and even more so under U.S. law (see 47 U.S.C. § 230[2656]). Similarly, software manufacturers also typically face no liability under U.S.

[2646] *See supra* chapter 5.4.2.

[2647] *See supra* chapter 5.2.2.2.

[2648] *See supra* chapter 5.1.1.

[2649] *See supra* chapter 5.1.2.

[2650] *See supra* chapter 5.1.3.

[2651] *See supra* chapter 5.1.4.

[2652] *See supra* chapters 5.1.5.1 to 5.1.5.4.

[2653] *See supra* chapter 5.1.5.5.

[2654] *See supra* chapter 5.1.6.

[2655] *See supra* chapter 5.2.1.2.

[2656] *See supra* chapter 5.2.1.1.

product liability law,[2657] U.S. law on express and implied warranties,[2658] the EU's Product Liability Directive[2659] or the Consumer Sales Directive.[2660]

Indirect risk transfers by way of mandatory disclosure of security-related information could be performed very effectively by data security breach notification policies or network security breach notification policies. However, both types of policies, as currently implemented in EU and U.S. law, are concerned with risk mitigation rather than performing a risk transfer.[2661] The only regulatory policy under EU law that performs an indirect risk transfer is the prohibition of misleading security claims about products and services (see Unfair Commercial Practices Directive article 6[2662]).[2663] Significantly, U.S. law does not only outlaw deceptive advertising (see FTC Act § 5,[2664] California Business and Professions Code § 17200, and New York General Business Law § 349[2665]) but also mandates the disclosure of certain vulnerabilities ("material weaknesses") by publicly traded companies (see SOX §§ 302, 404[2666]).

In sum, risk transfers are only performed to a rather limited extent by EU or U.S. law. Direct risk transfers by way of liability assignments are only performed in the area of payment

[2657] *See supra* chapter 5.3.1.

[2658] *See supra* chapter 5.3.2.

[2659] *See supra* chapter 5.3.3.

[2660] *See supra* chapter 5.3.4.

[2661] *Cf. supra*.

[2662] *See supra* chapter 6.4.3.

[2663] In stark contrast to SOX, the Statutory Audit Directive only requires the disclosure of "material weaknesses" to the audit committee but not to the public. *See supra* chapter 6.1.2.

[2664] *See supra* chapter 6.4.1.

[2665] *See supra* chapter 6.4.2.

[2666] *See supra* chapter 6.1.1.

services and, as far as the EU is concerned, electronic signatures. Indirect risk transfers are only performed in the area of deceptive advertising and, as far as the U.S. is concerned, financial reporting of publicly traded companies.

A comparison of the risk mitigation and risk transfer measures implemented in EU and U.S. law clearly shows that risk mitigation is the treatment option overwhelmingly chosen by policy makers in the EU the U.S. alike. Risk transfer measures are indeed rarely implemented in either EU or U.S. law. Furthermore, not a single regulatory policy adopts an approach based on risk avoidance.

8.2. Regulatory Focus on Actors of the Information Security Landscape

As discussed *supra* in chapter 2.3, the main actors of the information security landscape are (1) providers of communications services; (2) providers of online services; (3) software manufacturers; (4) other businesses, in particular in their capacity as personal information controllers; (5) consumers; (6) governments; and (7) malicious actors.

Providers of communications services (most significantly Internet access providers and Internet backbone providers) are subject to security requirements regarding personal information (see Communications Act § 222[2667] and ePrivacy Directive article 4[2668]) and, as far as EU law is concerned, regarding the availability of communications services and networks (see Telecoms Framework Directive article 13a[2669]). They are generally not exposed to liability for third-party content (see 47 U.S.C. § 230[2670] and E-Commerce Directive

[2667] *See supra* chapter 4.1.5.

[2668] *See supra* chapter 4.1.9.

[2669] *See supra* chapter 4.3.1.

[2670] *See supra* chapter 5.2.1.1.

article 12[2671]) or for security breaches (whether on a contractual[2672] or non-contractual basis[2673]). Communications service providers are further subject to mandatory data security breach notification (see Communications Act § 222[2674] and ePrivacy Directive article 4(3)[2675]) as well as mandatory network security breach notification (see FCC Network Outage Reporting Rule[2676] and Telecoms Framework Directive article 13a(3)[2677]).

Providers of online services, to the extent that they act as personal information controllers, have to implement security controls under both EU and U.S. law (see in particular FTC Act § 5[2678] and EUDPD article 17[2679]). U.S. law further specifically mandates the implementation of safeguards for children's personal information (see COPPA[2680]) and provides additional sector specific requirements (see HIPAA Security Rule,[2681] GLBA § 501(b),[2682] and FCRA[2683]). Also, U.S. law—but not EU law—subjects online service providers, in their capacity as personal information controllers, to mandatory data security breach notification.

[2671] *See supra* chapter 5.2.1.2.

[2672] *See supra* chapter 5.2.2.

[2673] *See supra* chapter 5.1 (generally discussing the liability of personal information controllers).

[2674] *See supra* chapter 6.2.6.

[2675] *See supra* chapter 6.2.9.

[2676] *See supra* chapter 6.3.1.

[2677] *See supra* chapter 6.3.2.

[2678] *See supra* chapter 4.1.6.

[2679] *See supra* chapter 4.1.8.

[2680] *See supra* chapter 4.1.4.

[2681] *See supra* chapter 4.1.1.

[2682] *See supra* chapter 4.1.2.

[2683] *See supra* chapter 4.1.3.

However, they generally do not face any liability for such breaches.[2684] Furthermore, under U.S. law, online service providers are generally not liable for any third-party content (see 47 U.S.C. § 230[2685]) while EU law provides a notice-and-takedown regime (see E-Commerce Directive article 14[2686]).

Software manufacturers only have to implement specific security requirements if the software in question is medical device software (see FFDCA § 520(f)[2687] and Medical Devices Directive annex I[2688]) or, under EU law, a certain type of signature product (see eSignature Directive annex III[2689]). They typically face no liability for the low levels of information security provided by their products that they cannot easily disclaim—neither under U.S. product liability law,[2690] U.S. law on express and implied warranties,[2691] the EU's Product Liability Directive[2692] nor the Consumer Sales Directive.[2693] Furthermore, they are also not subject to any measures that would perform an indirect risk transfer—besides a general prohibition of deceptive security claims about their products (see FTC Act § 5,[2694] California Business and Professions Code § 17200, New York General Business Law § 349,[2695] and

[2684] *See supra* chapter 5.2.2 (discussing contract-based liability of online service providers) and chapter 5.1 (generally discussing the non-contractual liability of personal information controllers).

[2685] *See supra* chapter 5.2.1.1.

[2686] *See supra* chapter 5.2.1.2.

[2687] *See supra* chapter 4.5.1.

[2688] *See supra* chapter 4.5.2.

[2689] *See supra* chapter 4.5.3.

[2690] *See supra* chapter 5.3.1.

[2691] *See supra* chapter 5.3.2.

[2692] *See supra* chapter 5.3.3.

[2693] *See supra* chapter 5.3.4.

[2694] *See supra* chapter 6.4.1.

Unfair Commercial Practices Directive article 6[2696]). In sum, software manufacturers are generally neither subject to the mandatory implementation of security controls, liability for "unsecure" software, nor the mandatory disclosure of security-related information.

Under U.S. law, businesses in general have to implement (largely sector-specific) security requirements to protect personal information (see HIPAA Security Rule,[2697] GLBA § 501(b),[2698] FCRA,[2699] FTC Act § 5(a),[2700] and various California and New York state laws[2701]). EU law establishes a single set of generally applicable requirements (see EUDPD article 17[2702]) which are, however, less stringent as some of the sector-specific instruments under U.S. law (in particular the HIPAA Security Rule). U.S. law—but not EU law[2703]—also mandates the implementation of security controls in the context of financial reporting (SOX §§ 302, 404[2704]). Under both EU and U.S. law, businesses generally face no liability for the types of damages typically caused by breaches of the security of personal information.[2705] However, U.S. law—but not EU law[2706]—generally requires them to perform a notification of

[2695] *See supra* chapter 6.4.2.

[2696] *See supra* chapter 6.4.3.

[2697] *See supra* chapter 4.1.1.

[2698] *See supra* chapter 4.1.2.

[2699] *See supra* chapter 4.1.3.

[2700] *See supra* chapter 4.1.6.

[2701] *See supra* chapter 4.1.7.

[2702] *See supra* chapter 4.1.8.

[2703] *See supra* chapter 4.2.2 (discussing Fourth Company Law Directive art. 46a).

[2704] *See supra* chapter 4.2.1.

[2705] *See supra* chapter 5.1.

[2706] The only data security breach notification regime currently implemented in EU law only applies to communications providers. *See* chapter 6.2.9 (discussing ePrivacy Directive art. 4(3)).

such breaches (see California Senate Bills 1386[2707] and 541,[2708] New York ISBNA,[2709] HITECH Act §§ 13402, 13407,[2710] and GLBA § 501(b)[2711]). In sum, businesses in general are significantly more regulated under U.S. law since they do not only have to implement security controls to protect personal information (compare EUDPD article 17) but also (1) have to implement security controls in the context of financial reporting; and (2) have to notify breaches of the security of personal information. In part, the increased regulatory attention paid to the security and, in particular, confidentiality of personal information can be explained by the fact that impersonation fraud is typically misconceived as "identity theft."[2712]

Consumers' obligations in the area of information security are rarely the subject of any regulatory policy in the EU or the U.S. Indeed, the only such regulatory policy is that limiting the liability of payment service users (see Truth in Lending Act § 133(a),[2713] Electronic Fund Transfer Act § 909(a),[2714] and Payment Services Directive article 61[2715]).

[2707] *See supra* chapter 6.2.1.

[2708] *See supra* chapter 6.2.2.

[2709] *See supra* chapter 6.2.3.

[2710] *See supra* chapter 6.2.4.

[2711] *See supra* chapter 6.2.5.

[2712] *See supra* chapter 4.1.10.1 (discussing the policy implications of this misconception). *Cf.* GINA MARIE STEVENS, CONG. RESEARCH SERV., DATA SECURITY: FEDERAL LEGISLATIVE APPROACHES, CRS REPORT FOR CONGRESS RL33273, at 1 (2007), *available at* http://epic.org/privacy/idtheft/RL33273.pdf (noting that the 109th Congress has spent considerable time assessing data security practices and working on data breach legislation "[b]ecause concerns about possible identity theft resulting from data breaches are widespread").

[2713] *See supra* chapter 5.4.1.

[2714] *See id.*

[2715] *See supra* chapter 5.4.2.

Federal government agencies are heavily regulated under U.S. law. Not only do they have to implement technical security controls pursuant to FISMA,[2716] they are also subject to mandatory data security breach notification (OMB Memorandum M-07-16[2717]). California and New York state governments also have to notify data security breaches (see California Senate Bills 1386[2718] and New York ISBNA[2719]). In stark contrast to the legal situation in the U.S., EU law does not impose any comparable security requirements or a breach notification obligation on EU institutions or Member State governments.[2720] However, it should be kept in mind that the European Commission is in size only about 2.7% of the executive branch of the U.S. federal government.[2721]

Lastly, malicious actors are covered by criminal law that aims to deter them from mounting certain computer-based information security threats. In the U.S., a significant number of computer crime statutes have been adopted (see CFAA,[2722] Wiretap Act,[2723] Stored Communications Act,[2724] California Penal Code § 502,[2725] and New York Penal Law

[2716] *See supra* chapter 4.4.1.

[2717] *See supra* chapter 6.2.8.

[2718] *See supra* chapter 6.2.1.

[2719] *See supra* chapter 6.2.3.

[2720] *Cf. supra* chapter 4.4.2 (discussing the Commission's and the Council's Rules of Procedure which only establish requirements for classified information).

[2721] *See id.*

[2722] *See supra* chapter 7.1.1.

[2723] *See supra* chapter 7.1.2.

[2724] *See supra* chapter 7.1.3.

[2725] *See supra* chapter 7.2.1.

§§ 156.05-35, 250.05[2726]) while the EU has only introduced a single such measure, the Framework Decision on Attacks Against Information Systems.[2727]

In summary, U.S. information security law most heavily regulates businesses in their capacity as personal information controllers or as publicly traded companies. Providers of communications services and online services as well as federal government agencies are also regulated to a significant, albeit lesser, extent. Malicious actors and, to some degree, consumers are also the subject of regulatory action. Lastly, software manufacturers—with the exception of medical device software manufacturers—face almost no regulatory requirements at all.

The legal situation in the EU is similar in the sense that, here too, software manufacturers do not receive any regulatory attention (with the exception of manufacturers of medical device software and certain signature software). The most heavily regulated actors are communications service providers which are currently subject to the EU's only data security breach notification regime. Providers of online services and other businesses are regulated to a lesser extent. Malicious actors and consumers have, so far, only received a comparatively small amount of regulatory attention. Furthermore, in contrast to U.S. law, EU law does not assign the EU's "federal government" or the Member States' governments a significant role as regards information security.

[2726] *See supra* chapter 7.2.2.

[2727] *See supra* chapter 7.3.

8.3. Meeting the Fundamental Challenges of Information Security

The following fundamental challenges of information security were identified *supra* in chapter 2.4: (1) the imperfection of technology; (2) the imperfection of people; (3) uninformed risk decisions and the difficulty of measuring security; and (4) the misalignment between risk and risk mitigation capability.

The imperfection of technology is a challenge that is rooted in the complexity of technology and in particular in that of software.[2728] This challenge can therefore not be entirely overcome by regulatory means. However, regulation can play a very important part in ensuring that technological products while being necessarily imperfect contain as few defects as reasonably possible. Most importantly, regulation may prescribe quality assurance and quality control measures to be implemented in the software development process. EU and U.S. law only require such measures for medical device software (see FFDCA § 520(f)[2729] and Medical Devices Directive annex I[2730]) and a certain type of signature product (see eSignature Directive annex III[2731]). Furthermore, neither EU nor U.S. law makes software manufacturers liable for "unsecure" software,[2732] creating a situation where they have few incentives to voluntarily implement quality assurance and quality control measures. US. and EU law rather focus on software users in the form of personal information controllers[2733] and, as far as U.S.

[2728] *See supra* chapter 2.4.1.

[2729] *See supra* chapter 4.5.1.

[2730] *See supra* chapter 4.5.2.

[2731] *See supra* chapter 4.5.3.

[2732] *See supra* chapter 5.3.

[2733] *See supra* chapter 4.1.

law is concerned, publicly traded companies[2734] and government authorities,[2735] requiring them to mitigate the risks created by imperfect technology. In sum, both EU and U.S. law only partly address the fundamental challenge of the imperfection of technology and unfortunately do so in a reactive rather than pro-active manner.

The imperfection of people is also a challenge that can hardly be overcome solely by regulatory means. However, this does not mean that this characteristic is irrelevant to the effectiveness of regulatory policies; to the contrary: Any regulatory policy has to take these imperfections into account if it is not to expect people to do the impossible. In particular, a regulatory regime that requires (or effectively necessitates) the performance of a risk assessment but does not take into account the problems people typically face when tasked with the assessment of risks,[2736] will lead to fundamentally flawed risk assessments being performed.[2737] Unfortunately this applies to a wide array of regulatory regimes for personal information controllers (see GLBA § 501(b)[2738], FCRA,[2739] FTC Act § 5,[2740] California Assembly Bill 1950,[2741] EUDPD article 17,[2742] and ePrivacy Directive article 4[2743]), publicly

[2734] *See supra* chapter 4.2.

[2735] *See supra* chapter 4.4.

[2736] *Cf. supra* chapter 2.4.2 (discussing some of the most significant problems people face when having to assess risks).

[2737] *See supra* chapter 4.1.10.4.

[2738] *See supra* chapter 4.1.2.

[2739] *See supra* chapter 4.1.3.3 (discussing FCRA § 697(b)) and chapter 4.1.3.4 (discussing FCRA § 623(e)).

[2740] *See supra* chapter 4.1.6.

[2741] *See supra* chapter 4.1.7.3.

[2742] *See supra* chapter 4.1.8.

[2743] *See supra* chapter 4.1.9.

traded companies (see SOX §§ 302, 404[2744]), communications service providers (see Telecoms Framework Directive article 13a[2745]), government authorities (see FISMA[2746]) and, to a minor extent, manufacturers of medical device software (see FFDCA § 520(f)[2747] and Medical Devices Directive annex I[2748]). In sum, neither EU nor US law sufficiently take the fundamental challenge of the imperfection of people into account.

The challenge posed by uninformed risk decisions and the difficulty of measuring security is largely caused by (1) insufficient security-related information about products and services being made publicly available; and (2) the fact that the measurement of security based on currently available information is not widespread.[2749] As regards the first issue, both EU and U.S. law prohibit deceptive advertising;[2750] but only U.S. law implements a policy that aims at actively establishing transparency vis-à-vis the general public. This policy is limited to the area of financial reporting of publicly traded companies (see SOX §§ 303, 404[2751]). U.S. law and, to a more limited extent, EU law further implement data security breach notification regimes.[2752] However, their purpose and effect is not to establish transparency but rather to serve as detective measures that enable reactive measures by individuals concerned (or

[2744] *See supra* chapter 4.2.1.

[2745] *See supra* chapter 4.3.1.

[2746] *See supra* chapter 4.4.1 (discussing FISMA which explicitly requires the performance of a risk assessment).

[2747] *See supra* chapter 4.5.1.

[2748] *See supra* chapter 4.5.2.

[2749] *See supra* chapter 2.4.3.

[2750] *See supra* chapter 6.4.

[2751] *See supra* chapter 6.1.1.

[2752] *See supra* chapter 6.2.

government authorities).[2753] Lastly, both EU and U.S. law also implement network security breach notification policies which, however, only require that a government authority—and not the public—be notified.[2754] In sum, U.S. law does little and EU law even less to ensure that sufficient security-related information about products and services is publicly available.

The second issue of underutilization of security measurement techniques based on the information that is currently available, is largely rooted in misconceptions about the concept, object, or methods of measurement.[2755] Neither EU nor U.S. law addresses this issue in any way. In sum, the fundamental challenge posed by uninformed risk decisions and the difficulty of measuring security is mostly ignored by the law of either jurisdiction.

Lastly, the challenge of the misalignment between risk and risk mitigation capability can be addressed either by direct or indirect risk transfer measures. However, as discussed *supra* in chapter 8.1, both EU and U.S. law only perform risk transfers to a rather limited extent.

In conclusion, EU law as well as U.S. law fail to fully address any of the fundamental challenges of information security. The following chapter will provide recommendations for how EU and U.S. law should be amended to better meet these fundamental challenges and ultimately bring about a more secure information society.

[2753] *Cf. supra* chapter 6.2.10.2.

[2754] *See supra* chapter 6.3.

[2755] *See supra* chapter 2.4.3.

9. Policy Recommendations

The confidentiality, integrity, and availability of information depend on various types of actors: providers of communications services, providers of online services, software manufacturers, other businesses (in particular in their capacity as personal information controllers), consumers, governments, and malicious actors.[2756] Accordingly, information security cannot be fundamentally improved by only altering the behaviour of a single type of actor, let alone by a single regulatory measure (e.g. making software manufacturers liable for vulnerabilities or making Internet access providers liable for malware).

In recognition of the complexity of the information security landscape, the recommendations set out below do not propose a single radical measure but rather a holistic web of balanced measures. Only in concert do the proposed measures have the potential to fundamentally improve the confidentiality, integrity, and availability of information. Unless noted otherwise, all the measures proposed below are equally applicable to EU law and U.S. law.

9.1. Personal Information Controllers

To address the information security risks to personal information, two regulatory risk treatment measures are proposed: First, as a means of indirect risk mitigation, personal information controllers should have to implement "appropriate" safeguards whereas appropriateness should be judged by a clearly defined qualitative risk assessment method (see *infra* chapter 9.1.1). Second, personal information controllers should be subjected to a data security breach notification regime that performs an indirect risk transfer by establishing "targeted transparency" (see *infra* chapter 9.1.2).

[2756] *See supra* chapter 2.3.

Lastly, to address the threat of impersonation fraud (misleadingly often referred to as "identity theft"),[2757] a liability regime for entities that furnish information to consumer reporting agencies is proposed (see *infra* chapter 9.1.3).

9.1.1. Requiring "Appropriate" Safeguards and Defining a Risk Assessment Method to Determine What is "Appropriate"

As a form of indirect risk mitigation, EU as well as U.S. law already require personal information controllers to implement safeguards.[2758] Such safeguard requirements are either of a general or a specific nature. As discussed *supra* in chapter 4.1.10.4, a policy that requires certain specific safeguards carries with it the risk that policy makers will mandate the implementation of ineffective safeguards or will fail to continuously update the regulatory requirements in reflection of rapidly changing circumstances.

General safeguard requirements, on the other hand, put the burden of performing a risk assessment and selecting the "appropriate" safeguards on the personal information controllers. However, the quality of the risk assessment methods currently used in practice varies greatly. Indeed, many of the assessment methods do not amount to more than an eyewash.[2759]

Both specific safeguard requirements as well as general safeguard requirements pose significant challenges. However, given that personal information controllers—even within the same industry sector—are very inhomogeneous as regards their capabilities and the types of personal information they process, a specific-safeguards-approach seems particularly ill

[2757] *Cf. supra* chapter 4.1.10.1.

[2758] *See supra* chapter 4.1.

[2759] *Cf. supra* chapter 4.1.10.4.

suited. Rather, policy makers should adopt a regulatory approach primarily based on requiring "appropriate" safeguards.

To address the difficulty of determining appropriateness, policy makers should identify a particular risk assessment method to be used. As demonstrated *supra* in chapter 4.1.10.4, such a method should (1) be quantitative in nature so that it can produce verifiable results; (2) clearly express uncertainty; (3) address the psychological challenges humans face when estimating risks; and (4) provide guidance for how to measure a risk's potential impact on personal information.

Since the development of such a method is very challenging, policy makers should approach the problem in a three-step process: (1) funding research and standardization efforts; (2) assessing the quality of the emerging risk assessment standards; and (3) mandating the use of a specific standard for enforcement purposes.

In particular smaller businesses may find it too burdensome to perform an entire risk assessment. Accordingly, the performance of a risk assessment should not be mandatory. However, since "appropriateness" would be eventually judged in light of a risk assessment performed by the enforcement authority, personal information controllers would have to perform such an assessment themselves if they want to determine whether they are in compliance.

The following regulatory measures currently require the implementation of "appropriate" or "reasonable" safeguards and would greatly benefit from a clearly defined risk assessment method: the regulations promulgated pursuant to GLBA § 501(b),[2760] FCRA § 697(b),[2761] the

[2760] *See supra* chapter 4.1.2.

Furnishers Rule promulgated pursuant to FCRA § 623(e),[2762] FTC Act § 5,[2763] California Assembly Bill 1950,[2764] EUDPD article 17,[2765] and ePrivacy Directive article 4.[2766]

Ideally, the EU and the U.S. would agree on a single such standard for both jurisdictions. This would not only lessen the burden for businesses that operate in the EU as well as the U.S., it would also create legal certainty as regards online services provided across jurisdictional boundaries.

9.1.2. Universally Applicable Data Security Breach Notification

Data security breach notification regimes currently implemented in U.S. and EU law are concerned with mitigating risks by allowing the individuals concerned to take reactive measures to a breach. However this approach is fundamentally flawed for a number of reasons which are discussed *supra* in chapter 6.2.10.2. Data security breach notification policies should rather focus on performing an indirect risk transfer by creating "targeted transparency."[2767]

Breach notifications have the potential to serve as much-needed indicators for the level of security provided by different personal information controllers.[2768] Such indicators would

[2761] *See supra* chapter 4.1.3.3.

[2762] *See supra* chapter 4.1.3.4.

[2763] *See supra* chapter 4.1.6.

[2764] *See supra* chapter 4.1.7.3.

[2765] *See supra* chapter 4.1.8.

[2766] *See supra* chapter 4.1.9.

[2767] *See supra* chapter 3.2.3.2 (discussing the fundamentals of targeted transparency policies as defined by ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY (2007)).

[2768] *Cf. supra* chapter 2.4.3 (discussing the fundamental challenge of uninformed risk decisions); ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 61 (2008) (noting that objective data that would enable good security decisions is in short supply). *Cf. also* Kathryn E. Picanso, *Protecting* allow individuals to base decisions about who to trust their personal information with on the relative security of personal information controllers. In particular, individuals could use such security indicators to decide whether to change to a competitor or, in the case where the individual concerned is not a customer of the controller, request that his personal information be deleted (if such a right exists under applicable law).[2769] Thus, by allowing individuals to make more informed risk decisions, controllers would ultimately face financial losses should they fail to provide sufficient security for personal information.[2770] To indeed effect such an indirect risk transfer, a data security breach notification policy has to ensure that the breach information becomes "embedded" in the decision-making processes of individuals. This requires (1) that users perceive the breach information to have value for achieving higher levels of security for their information;[2771] (2) that the breach information is compatible with individuals' decision-making processes in particular with regard to the information's format and its time and place of availability;[2772] and (3) that the breach information is easily comprehensible for individuals.[2773]

Information Security Under a Uniform Data Breach Notification Law, 75 FORDHAM L. REV. 355, 360 (2006) (stating that more data on security breaches is essential to improving overall information infrastructure protection).

[2769] *Cf.* EUDPD art. 12(b).

[2770] *Cf.* Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?,* 43 HOUS. L. REV. 1597, 1631 (2007) (stating that mandatory breach notifications inflict on businesses costs associated with both a tarnished image and the expense of providing notice, thereby providing more motivation for companies to ensure proper consumer data protection).

[2771] *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 55 (2007).

[2772] *Cf. id.* at 56.

[2773] *Cf. id.* at 59.

The first requirement prompts the question which security breaches should be subject to mandatory notification.[2774] Breaches of the confidentiality or integrity of personal information are always relevant for the affected individuals. Breaches of availability, on the other hand, are generally not equally significant. More precisely, information availability will only be a major concern to individuals if the information is maintained for their benefit.[2775] For example, whether personal information used by a company for marketing purposes (i.e. for the company's benefit) is unavailable (to the company) for a certain time or even destroyed does not matter to the individuals concerned. If on the other hand, a company offers online data storage to its users (i.e. maintains information for the users' benefit), users would want to know if their information was temporarily unavailable or even destroyed.

Contrary to most of the notification regimes currently implemented in U.S. and EU law,[2776] a breach notification should not depend on whether there is a risk of *future* harm. A breach itself already constitutes a harm which the individuals concerned would want to know about and, more importantly, has great potential to influence decisions as to whom to entrust their personal information.

A breach of confidentiality, integrity, and/or availability should be presumed to have occurred if (1) somebody gained "unauthorized access" to the information or (2) as regards confidentiality, if the information was subject to an "unauthorized disclosure." In comparison,

[2774] *Cf. supra* chapter 6.2.10.3 (discussing how existing regulatory measures answer this question).

[2775] This limitation resembles the requirement under the FTC Health Breach Notification Rule that, for information to be covered, it has to be "managed, shared, and controlled by or primarily for the individual." *See* HITECH Act § 13400(11), 42 U.S.C. § 17921(11); 16 C.F.R. § 318.2(d) and (e). *Cf. supra* chapter 6.2.4.2.

[2776] The following breach notification regimes only require the notification of the individuals concerned if there is a risk of harm: the HHS Breach Notification Rule (*see supra* chapter 6.2.4.1), the regulations issued under GLBA § 501(b) (*see supra* chapter 6.2.5), the VA Breach Notification Rule (*see supra* chapter 6.2.5), OMB Memorandum M-07-16 (*see supra* chapter 6.2.8), and ePrivacy Directive art. 4(3) (*see supra* chapter 6.2.9).

a notification trigger based on "unauthorized acquisition," would have the disadvantage that an acquisition of information is rather difficult to detect.[2777]

It should be possible to rebut a presumption created by an "unauthorized access" or "unauthorized disclosure" if safeguards were in place that prevented an actual breach. For example, a strong encryption process that has not been compromised[2778] could preserve confidentiality in the event of an unauthorized access to the (encrypted) information. Also, cryptographic one-way hash functions[2779] could be used to verify that no information has been altered or deleted. As regards temporary unavailability (e.g. the time period until a service recovers from a malfunction or until destroyed information is restored from a backup), no presumption can be provided. A covered entity would have to rely on its own resources and on user reports to determine whether and for how long personal data was unavailable.

In summary, to fulfill the first requirement of ensuring that users perceive the breach notifications to have value for achieving higher levels of security for their information, a data security breach notification policy should cover breaches of confidentiality, integrity, and—if the information was maintained for the benefit of the individual—availability, irrespective of a risk of harm. Such a breach should be presumed to have occurred in cases of "unauthorized access" and "unauthorized disclosure." However, controllers should be able to rebut this presumption by proving that safeguards were in place which prevented an actual breach.

[2777] *Cf. supra* chapter 6.2.10.3.

[2778] This requires that the encryption algorithm has not been "cracked" and that the decryption key has not been compromised. *Cf. supra* chapter 6.2.10.3.

[2779] *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 429 et seq. (2d ed. 1996).

The second requirement noted above is to ensure that the breach information is compatible with individuals' decision-making processes in particular with regard to the information's format and its time and place of availability. To meet this requirement (and to increase the perceived value of the breach information), individuals have to be able to compare information about different controllers at the time they choose to trust a particular controller with their personal information. Such a comparison is not possible if breach notifications are not publicly available from a central repository. Accordingly, controllers should have to notify a government agency that maintains such a central online repository. That repository should make all notices available in easily accessible (e.g. HTML) as well as structured data formats (e.g. XML).[2780] Furthermore, customizable push technology (e.g. e-mail) should be used so that individuals (e.g. a reporter) can choose to get informed of breaches that meet specific criteria.

It has to be stressed that, to be effective in performing a risk transfer, such a central repository has to be maintained on a federal level.[2781] This means that for the U.S., an agency of the federal government and for the EU, an agency of the European Commission should be in charge of maintaining the central repository. However, in particular with regard to the EU, such an agency can be of a non-regulatory nature. Building on the current enforcement mechanisms of the Data Protection Directive, enforcement of an EU data security breach notification regime should remain in the hands of the Member States whereas a non-

[2780] In this regard, the National Vulnerability Database operated by the National Institute of Standards and Technology (NIST) serves as an excellent example. It offers the entire database for download as an XML file. *See* http://nvd.nist.gov/download.cfm (last accessed Feb. 10, 2011).

[2781] A common repository for the EU and the U.S. would of course be even more beneficial but seems highly unrealistic for political reasons.

regulatory agency such as the European Network and Information Security Agency (ENISA)[2782] could operate the central breach repository.

In this context, the following question should be raised: What is the importance of notifications to the individuals concerned in relation to the importance of government notification, taking into account in particular that the former are perceived by controllers as very burdensome.

Since the proposed data breach notification policy does not focus on helping to mitigate risks resulting from a breach, individual notifications clearly take a back seat to the notification of the government agency that will make the notification publicly (and permanently) available. However, this does not mean that controllers should not be required to also notify the individuals concerned. Indeed, the compatibility with individuals' decision-making processes may be significantly increased by the additional awareness raised by individual notifications for information security in general and for the existence of a central breach repository in particular. Furthermore, albeit unrelated to the effectiveness of the risk transfer, it could be argued that to the extent information privacy is recognized as a fundamental right,[2783] individuals should have a right to be notified of any interference with such right.[2784]

Ultimately, individual notifications are a necessary element of a breach notification policy but are only a secondary priority. In this regard it is important to recognize that individual

[2782] *See* Parliament and Council Regulation 460/2004, 2004 O.J. (L 77) 1 (EC) (establishing ENISA); Parliament and Council Regulation 1007/2008, 2008 O.J. (L 293) 1 (EC) (extending ENISA's mandate until Mar. 14, 2012).

[2783] *Cf.* Charter of Fundamental Rights of the European Union, art. 8, 2010 O.J. (C 83) 389, 393; CAL. CONST. § 1.

[2784] *Cf.* Ann Florini, *Introduction: The Battle Over Transparency, in* THE RIGHT TO KNOW: TRANSPARENCY FOR AN OPEN WORLD 1, 3 (Ann Florini ed., 2007) (remarking generally that "[a] human rights argument combines pragmatic and moral claims, seeing access to information as both a fundamental human right and a necessary concomitant of the realization of all other rights").

notifications may be very costly, depending in particular on the required method of notification. This may create substantial financial disincentives for complying with the entire notification regime. To realize the benefits of individual notifications while, at the same time, minimizing its potential negative effects on the policy's general effectiveness, the required method of individual notification should be as cheap as possible. Specifically, it should be sufficient if the individuals concerned are notified—irrespective of prior consent—via an individual electronic message (e.g. e-mail) in combination with a posting on the homepage of the website of the controller. Expensive methods of notification like regular mail or paying for notices to be published in the media should not be mandatory. Such low requirements regarding the method of notification will not ensure that all individuals receive a notification. However, this will be offset by the higher rate of compliance that can be expected due to the less expensive notification methods.

The third requirement of ensuring that the breach information is easily comprehensible for individuals is particularly challenging. It necessitates not only the prescription of certain information items to be included in any breach notification, but also that the government agency that maintains the central breach notification repository develops metrics to better communicate the level of (personal) information security provided by a certain controller.

To be comprehensible to laypersons while at the same time providing more detailed information for more experienced individuals and experts, a data security breach notification should contain at least the following information items:

First, a description of the breach in lay terms: The cause of the breach as well as its effects on the information should be described in an easily understandable manner. The description of the cause of the breach should be specific enough so as to give individuals a general idea of what happened. The effects of the breach should specifically state whether and to what extent the information's confidentiality, integrity, and/or availability was compromised.

Second, a reference (including a URL) to the central breach repository maintained by the government agency: This will help to raise awareness for and to actually locate the central breach repository.

Third, the date of the breach and the date of its discovery: How long it takes a controller to discover a breach is an important indicator for the controller's incident detection capabilities.

Fourth, a description of the breach in technical terms: In particular, this means that not only the threat that materialized in the breach (e.g. a specific malware) but also the vulnerability it managed to exploit has to be described (i.e. the vulnerability's CVE Identifier[2785] or, if none has been assigned, a description of the vulnerability along with a CWE Identifier[2786]).

Fifth, an estimate of the number of individuals affected: This item is essential to estimate the significance of the breach. Remarkably, none of the notification regimes implemented in the U.S. and the EU require this information to be disclosed to individuals.[2787]

Sixth, a description of the group of individuals affected: This will help individuals to determine whether their data was affected even if they do not receive an individual notification via e-mail but learn about the breach from a public source. Such a group could,

[2785] CVE (Common Vulnerabilities and Exposures) Identifiers are unique, common identifiers for publicly known information security vulnerabilities. *See* http://cve.mitre.org/cve/identifiers/index.html (last accessed Feb. 10, 2011). The CVE Initiative is sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security. *See* http://cve.mitre.org (last accessed Feb. 10, 2011).

[2786] CWE (Common Weakness Enumeration) Identifiers are unique, common identifiers for *types* of software vulnerabilities. This also includes vulnerabilities caused by the software's configuration or its environment for which CVEs are typically not available. *See* http://cwe.mitre.org/about/index.html (last accessed Feb. 10, 2011).

[2787] *See supra* chapter 6.2.10.2.

for example, be defined as all customers of the controller who have a membership card or all individuals who used a certain service offered by the controller within a certain time frame.

Seventh, the types of information affected: Since electronic information is typically stored in a structured form (e.g. in a relational database), it should be easy to identify the various information types (e.g. credit card number, name and shipping and billing address for all customers).

Eighth, the quantity of information affected in terms of its maximum and minimum age: Some companies might retain personal information only for a very limited time while others—in particular if governed by U.S. law—might never delete it.

It should be noted that the above list would not require an entity to disclose the safeguards in place prior to the breach or the actions taken in response to the breach. This is because information regarding safeguards could often be considered a trade secret providing a competitive advantage to the controller. So as not to reduce competition with regard to information security, safeguard-related information should not have to be disclosed. The vulnerabilities, however, that were exploited in course of the breach, cannot be considered a trade secret and should therefore be subject to mandatory disclosure.

As mentioned above, to ensure that the breach information is easily comprehensible for individuals, a security metric should be developed that expresses the level of (personal) information security provided by a certain controller in simple terms. It has to be acknowledged that such a breach-based metric is by no means perfect. However, given that individuals currently have only very little information by which to judge the security of controllers, a perfect measurement is not needed to significantly reduce uncertainty.[2788] The metric should be based on the number and type of security breaches suffered by a controller, whereas the relevance of each breach should decrease over time. The result of the calculations should be expressed as a simple grade (e.g. one to five or one to ten), possibly supported by color codes.[2789]

As regards the personal scope of application of a data security breach notification policy, it is important not to disregard the fact that many information processing operations are being outsourced by personal information controllers. Since outsourcing should not allow the controller to avoid knowledge of a breach, personal information processors should be required to notify the controller of all breaches and to obtain and preserve a confirmation of receipt. This has the important benefit over simply mandating provisions in outsourcing contracts that the processors are also subject to public enforcement.

The personal scope of application should also not be sector-specific.[2790] If reporting requirements would differ from sector to sector, an analysis of all breach notifications would

[2788] *Cf.* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 110 (2d ed. 2010) (emphasizing that it is often assumed that if there is a lot of uncertainty, a lot of measurement data is needed to reduce it while, in fact, just the opposite is true).

[2789] *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 59 (2007) (discussing the importance of making information comprehensible for users). *Cf. also* Parliament and Council Directive 2010/30, art. 10(4)(d), 2010 O.J. (L 153) 1, 7 (EU) (mandating the use of a color scale to inform end-users about products' consumption of energy whereas the color scale "shall consist of no more than seven different colours from dark green to red").

[2790] *Cf.* ROSS ANDERSON ET AL, SECURITY ECONOMICS AND THE INTERNAL MARKET 26 (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport (recommending that data security breach notification legislation be passed in the EU that covers all sectors of economic activity); Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1116 (2009) (arguing against a sector-specific approach, stating that factors such as "the relationship of the individuals to the organization" or "an understanding of the information needs of the organization" are not relevant because unauthorized release, theft, or loss of information was the common problem regardless of these factors); NEIL ROBINSON ET AL, REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 43 (2009), *available at* http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf (proposing the introduction of limited require that the particularities of each sector-specific regulation be taken into account. A comparison of one sector to another would also be more difficult.[2791] Indeed, as demonstrated by California Senate Bill 1386 and New York ISBNA, no sector-specific approach is needed.

Lastly, the EU's challenges of multilingualism has to be addressed. If each company issues its breach notifications in the official language of the Member State having jurisdiction,[2792] it would be very costly for the EU agency in charge of maintaining the central breach repository to translate all breach notifications into all other 22 official languages of the EU.[2793] To not provide any translated versions of the notifications would make it practically impossible for individuals to get informed about the specific "breach history" of a controller that is established in a Member State whose official language they do not speak. To at least partly overcome this challenge, the following pragmatic solution is proposed: All breach notifications—whether addressed to an individual or a public authority—should be issued in two languages, the official language of the Member State having jurisdiction and English. While politically a difficult issue in the EU,[2794] English is nevertheless understood best as a

breach notification obligations for all data controllers). *Cf. also supra* chapter 4.1.10.2 (discussing certain aspects of sector-specificity).

[2791] *Cf., e.g.,* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches,* 105 MICH. L. REV. 913, 964 (2007) (emphasizing the importance of comparative statistical information regarding data security events).

[2792] If a data security breach notification policy was implemented in the EU, it would be advisable to do so in the context of the current data protection framework. In that case, jurisdiction would depend on where the controller is established. *See* Data Protection Directive art. 4(1)(a) (stating that a Member State's national data protection law is applicable if "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State"). *Cf.* EUGEN EHMANN & MARCUS HELFRICH, EG DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE] 100 et seq. (1999).

[2793] *Cf.* Council Regulation No. 1/1985, 1958 O.J. (17) 385 (EEC) as amended (stating that the official languages of the institutions of the Union are Bulgarian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovene, Spanish, and Swedish).

[2794] *Cf., e.g.,* Ulrich Ammon, *Language conflicts in the European Union*, 16 INT'L J. OF APPLIED LINGUISTICS 319 (2006).

second language by a relative majority of EU citizens.[2795] Those individuals that do not understand either of the two languages in which notifications are available would have to rely on the metric calculated by the agency.

9.1.3. Addressing "Identity Theft": Making Creditors Liable for Failing to Perform Strong Authentication of Credit Seekers

"Identity theft" describes a fraud committed by using the identifying information of another person without authority. As discussed *supra* in chapter 4.1.10.1, this phenomenon hardly exists in the EU while it is a major concern in the U.S. The policy proposal set out below therefore only addresses the legal situation in the U.S.

The term "identity theft" wrongly suggests that the challenge would be to deter, prevent, and detect the "theft" of identifying information, that is, to increase the level of confidentiality of identifying information. Attempting to keep identifying information confidential is, however, an impossible undertaking: For identifying information to be of any use, it necessarily has to be shared with others.[2796]

Once the problem is conceived as "impersonation fraud" rather than "identify theft," it becomes clear that the real challenge is proper authentication of credit seekers. The risks faced by the primary victim of the fraud (the creditor) are entirely under its control and therefore do not require any regulatory risk treatment. However, creditors typically cause secondary damages to the impersonated consumer when they inform consumer rating

[2795] *See* EUROPEAN COMM'N, EUROPEANS AND THEIR LANGUAGES 12 (2006), *available at* http://ec.europa.eu/public_opinion/archives/ebs/ebs_243_en.pdf (stating that English remains the most widely-spoken foreign language throughout Europe; 38% of EU citizens stated that they hade sufficient skills in English to have a conversation while only 14% stated the same about German or French).

[2796] *Cf. supra* chapter 4.1.10.1 (discussing the distinction between identification and authentication).

agencies that the consumer (who is wrongly believed to be the credit user) defaulted on his or her loan. This may in turn result in less favorable credit terms for the impersonated consumer or might even make it impossible for him or her to obtain a loan.

More precisely, the challenge is to ensure that creditors do not furnish negative information about a consumer unless he or she has been subjected to a strong authentication procedure. The introduction of a general obligation to better authenticate credit seekers, e.g. by amending USA PATRIOT Act § 326(a), would go beyond addressing that challenge as such an obligation would also apply when no information is to be furnished to consumer rating agencies. A general prohibition of the furnishing of information to consumer reporting agencies if the credit seeker has not been properly authenticated would have the appropriate scope but would (1) entirely rely on public enforcement for its effectiveness and (2) would risk challenges under First Amendment since it would constitute a form prior restraint.[2797]

Rather, a strict liability regime should be introduced that makes furnishers (i.e. entities that furnish information to a consumer reporting agency) liable for any damages (material, purely economic, or immaterial) caused by the reporting of information relating to a fraudulent transaction which was executed without having used strong authentication procedures to verify the identity of the credit seeker.[2798] Specifically, a creditor should have to perform two-factor authentication (e.g. using a government-issued photo ID). To not only address new

[2797] *Cf.* Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976) ("prior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights"); New York Times Co. v. United States, 403 U.S. 713, 714 (1971) ("Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity." (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963))).

[2798] A strict liability regime, albeit without a safe haven for lenders that perform strong authentication, has also been proposed by Chris Jay Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J. L. TECH. 2, 29 et seq. (2009), *available at* http://lawtechjournal.com/articles/2009/02_100406_Hoofnagle.pdf.

account fraud but also existing account fraud, lenders would have to perform a two-factor authentication before establishing a business relationship as well as before the execution of every credit transaction.[2799]

This would not prohibit any business practices that rely on weak authentication (e.g. granting credit to individuals who do not have a government-issued photo ID). It would also not subject creditors to any liability for these practices—as long as they do not furnish any information related to unauthenticated transactions to consumer reporting agencies.

9.2. Software Manufacturers

To better align risk and risk mitigation capability as regards software manufacturers and software users, three different measures are proposed: To perform a direct risk transfer, a statutory manufacturer warranty for vulnerability-free software (see *infra* chapter 9.2.1) as well as product liability in case of material damages (see *infra* chapter 9.2.2) should be implemented. Additionally, a common risk-based software security metric should be adopted (see *infra* chapter 9.2.3). This third measure will also greatly help individuals as well as businesses to make more informed risk decisions as to which software products to use.

[2799] The Federal Financial Institutions Examination Council (FFIEC), a federal interagency body empowered to prescribe uniform principles, standards, and report forms for use by the Board of Governors of the Federal Reserve System, the FDIC, NCUA, OCC, and OTS, has stated in a guidance that "single-factor authentication [is] inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties" if it is used "as the only control mechanism." FED. FIN. INSTS. EXAMINATION COUNCIL [FFIEC], AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 1 (2005), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf. The FFIEC is currently considering recommending more explicitly the use of two-factor authentication. *See* Jaikumar Vijayan, *Banks may soon require new online authentication steps*, COMPUTERWORLD, Jan. 25, 2011, http://www.computerworld.com/s/article/9206158/Banks_may_soon_require_new_online_authentication_steps?taxonomyId=82. *Cf. also* Bruce Schneier, *Is two-factor authentication too little, too late? It's not enough*, NETWORK WORLD, Apr. 4, 2005, http://www.networkworld.com/columnists/2005/040405faceoff-counterpane.html (emphasizing the importance of authenticating transactions rather than individuals). For example, some banks in the EU use a regular password as the first factor (something you know) and the user's cell phone (something you have) as a second factor by sending a one-time password needed to authorize a particular transaction via text message.

9.2.1. Statutory Manufacturer Warranty for Vulnerability-Free Software

Commentators regularly argue for making software manufacturers liable for security vulnerabilities.[2800] A direct risk transfer is indeed necessary to address the challenge of the misalignment between risk and risk mitigation capability, as it particularly applies to software.[2801] However, great care must be taken so as not to impose too much liability on software manufacturers. Consumers typically suffer large pure economic losses but rarely property damages or personal injuries due to low levels of software security.[2802] If the recovery of pure economic losses was generally permitted, software manufacturers would face huge financial risks[2803] that, due to the size of the risks, might be impossible to insure against.[2804] However, if pure economic losses cannot be recovered, as it is currently the case,[2805] software manufacturers only bear a very small portion of the risks associated with software vulnerabilities. As a remedy, the recovery of damages is therefore ill-suited as it does either too much or to little to transfer risk to software manufacturers.

[2800] Most famously, this argument is advanced by Bruce Schneier. *See* Bruce Schneier, *Make Vendors Liable for Bugs*, WIRED, June 6, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/06/71032, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 147 (2008). In particular *Schneier* does not consider a refund of the licensing fee sufficient, demanding "real liability" (apparently meaning liability for economic losses). Bruce Schneier, *BitArmor's No-Breach Guarantee*, SCHNEIER ON SECURITY, Jan. 23, 2009, http://www.schneier.com/blog/archives/2009/01/bitarmors_no-br.html.

[2801] *Cf. supra* chapter 2.4.4.

[2802] *Cf.* Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 302 (2006) (discussing various types of economic losses typically suffered due to software system security breaches).

[2803] For example, the worm Code Red is estimated to have caused $2.6 billion and the worm Blaster $2 to 10 billion in damages. *See* George Jones, *The 10 Most Destructive PC Viruses Of All Time*, INFORMATIONWEEK, July 5, 2006, http://www.informationweek.com/news/windows/security/showArticle.jhtml?articleID=190300173.

[2804] Rainer Böhme & Gaurav Kataria, *On the Limits of Cyber-Insurance*, *in* TRUST AND PRIVACY IN DIGITAL BUSINESS 31 (Simone Fischer-Hübner et al. eds., 2006) (showing that there may not be a market solution for globally correlated risks from the worldwide spread of a worm or virus, as the insurer's cost of safety capital becomes too high).

[2805] *See supra* chapter 5.3.

The Consumer Sales Directive suggests an alternative hierarchy of remedies that, if applied to software manufacturers, would perform a measured risk transfer. First, the Consumer Sales Directive allows the consumer to require a repair (or a replacement) of the good. Second, it allows the consumer to not only demand the (often impractical) rescission of the contract[2806] but, alternatively, to require a reduction of the price.[2807] It is this last remedy that is particularly well suited to transfer an adequate amount of risk from consumers to software manufacturers.

However, as discussed *supra* in chapter 5.3.4, the Consumer Sales Directive's regulatory regime is ultimately inadequate to transfer risk to software manufacturers: First, the Consumer Sales Directive does not apply to software that is not distributed on a tangible medium like a CD.[2808] Second, the relevant provisions of the Consumer Sales Directive only apply to sellers but not to manufacturers.[2809] Third, the availability of the Consumer Sales Directive's remedies largely depends on whether the consumer's "reasonable" expectations regarding the quality of the goods are met. Since software is generally known to contain countless security vulnerabilities, a "reasonable expectation"-standard rarely results in liability for software goods.[2810]

[2806] The costs of switching from one particular software product to another are often considerable. *Cf.* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 50 et seq. (2008). *Cf. also* chapter 2.3.3 (discussing the lock-in effects of software products).

[2807] *See supra* chapter 5.3.4.3 (discussing the remedies under the Consumer Sales Directive).

[2808] Even if software is distributed on a tangible medium, the Consumer Sales Directive's application remains questionable. *See supra* chapter 5.3.4.1.

[2809] *See id.*

[2810] *See supra* chapter 5.3.4.2.

The EU and the U.S. should introduce a statutory manufacturer warranty, breaches of which are subject to a liability regime that provides the same remedies as the Consumer Sales Directive but addresses the deficiencies identified above: Such a regime should cover all types of commercial off-the-shelf software, irrespective of whether or not it was distributed on a tangible medium. It should apply to manufacturers rather than "sellers," thereby avoiding the question under which circumstances a license can be considered a sale.[2811] Furthermore, to change the status quo of software security, an absolute standard—in addition to a standard based on "reasonable expectations"—should be used to determine whether the warranty has been breached. This absolute standard should be the total absence of any security vulnerabilities which are publicly known at the time the software is delivered or which become publicly known at any later time.

Such a high standard might seem excessive at first glance. However, the limited hierarchy of remedies ensures that the resulting risk transfer is only of a moderate nature. If a vulnerability in a software is publicly reported, the software would become deficient, giving the consumer the right to require a repair (or a replacement) of the software within a reasonable time (i.e. that a security update is provided). This means that the software manufacturer can fulfill all its obligations under the statutory warranty by providing security updates to all consumers within

[2811] Indeed, the European Commission has been considering whether to extend the Consumer Sales Directive's liability regime to producers. *Green Paper on the Review of the Consumer Acquis*, at 30, COM (2006) 744 final (Feb. 8, 2007) (noting that an application of the Consumer Sales Directive's remedies to producers "would eliminate possible internal market barriers and would favour especially consumers buying cross-border" and referring to the "Report on the implementation of the Consumer Sales Directive"); *Commission Communication on the implementation of Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees including analysis of the case for introducing direct producers' liability*, at 11, COM (2007) 210 final (Apr. 24, 2007) (stating that the Commission will examine the case for introducing direct producers' liability and, if appropriate, submit a proposal); Consumer Sales Directive recital 23 (stating that "it may be necessary to envisage more far-reaching harmonisation, notably by providing for the producer's direct liability for defects for which he is responsible"). *Cf. also* MICHAEL HASSEMER, HETERONOMIE UND RELATIVITÄT IN SCHULDVERHÄLTNISSEN [HETERONOMY AND RELATIVITY IN OBLIGATIONS] 167 (2007) (describing the two opposing schools of thought on this issue).

a reasonable time. Consumers will only have the right to demand a "reduction of the price" (i.e. payment of a sum that corresponds to an appropriate share of the price paid to the licensor or seller who may or may not be identical with the manufacturer) if the software manufacturer does not provide security updates within a reasonable time.

What constitutes a "reasonable" time should have to be determined based on the difficulty of developing a patch for the security vulnerability and its severity as expressed using a common standard such as the Common Vulnerability Scoring System (CVSS).[2812]

Furthermore, the regulatory regime would have to answer the question of how long the statutory warranty should remain valid, that is, for how long software manufacturers effectively have to provide patches for their old products. In this regard it has to be acknowledged that certain types of software products have a very long life cycle (e.g. operating systems)[2813] while others do not (e.g. web browsers).[2814] Since product-type-specific time limits are impractical, the following method of calculating the applicable time limit is proposed: two years as from the last delivery of the software to any consumer by an authorized distributor or the manufacturer itself but no longer than three years as of the last delivery of the software to any authorized dealer by the manufacturer.

[2812] For an introduction see Peter Mell et al., *Common Vulnerability Scoring System*, IEEE SECURITY & PRIVACY, Nov. 2006, at 85. *See also* PETER MELL ET AL., A COMPLETE GUIDE TO THE COMMON VULNERABILITY SCORING SYSTEM VERSION 2.0 (2007), *available at* http://www.first.org/cvss/cvss-guide.pdf. *Cf. also* http://nvd.nist.gov/cvss.cfm (last accessed Feb. 10, 2011).

[2813] Windows XP was first released in 2001 and will be supported (with Service Pack 3 or Service Pack 2 for 64 bit architectures) until Apr. 2014. *See* http://support.microsoft.com/lifecycle/?LN=en-us&x=12&y=7&C2=1173 (last accessed Feb. 10, 2011).

[2814] The different versions of Microsoft Internet Explorer were typically supported for two or three years. *See* http://support.microsoft.com/gp/lifesupsps/#Internet_Explorer (last accessed Feb. 10, 2011).

This will create the same time limit for all users instead of a user-specific time limit based on when each user received his or her software. This approach is appropriate given that the development and distribution of a software patch is characterized by very high fixed costs but marginal costs that are effectively $0. By re-starting the two-year-clock every time the software is delivered to a consumer, the time limit of the statutory warranty will effectively depend on the length of the life cycle of the software. To eliminate the risk that a distributor might intentionally prolong the manufacturer warranty by ordering 100 copies and selling one to a consumer each year, the warranty should expire, in any event, three years after the software manufacturer made its last delivery of the software to an authorized dealer.

It should also be noted that it is very costly for a software manufacturer to develop patches for multiple versions of its product (e.g. 1.0, 2.0, and 3.0). Indeed, it may be significantly cheaper for a software manufacturer to make all its users upgrade to the newest version for free (e.g. from 1.0 and 2.0 to 3.0) and to only provide security updates for that newest version. While this may create disincentives to install security updates for users wishing to continue to use the old version,[2815] it potentially reduces the manufacture's costs to a very significant extent. Accordingly, a software manufacturer should be allowed to combine security updates with feature updates.

In sum, this absolute standard for determining if the statutory manufacturer warranty was breached would reduce the consumers' information security risks by ensuring that (1) security updates are made available in a timely fashion or (2) the manufacturer repays an appropriate

[2815] *Cf.* ROSS ANDERSON ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET 64 (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport (arguing that the installation of updates that combine security patches and new feature are a nuisance for consumers since "[f]eature updates could disrupt customisation, slow down performance, or add undesirable features").

amount of the price initially paid for the software. At the same time, this increases the software manufacturers' risks related to security vulnerabilities of their products because they will have to use their resources to develop and distribute security updates more quickly than they might have in the past—or face requests for price reductions. Since fixing security vulnerabilities after a software has been released is typically much more expensive for the manufacturer than fixing them during the design, implementation, or testing phase,[2816] it is to be expected that manufacturers would increasingly focus on software quality assurance, thereby reducing the number of security vulnerabilities created in the first place.

This direct risk transfer is also aided by a "reasonable expectations"-standard which should apply in addition to the absolute standard described above. In particular it could be argued that there is a reasonable expectation that all consumer software implements an automatic update feature that is enabled by default.

As described so far, the statutory warranty only applies if the consumer exchanged anything of value for the software.[2817] However, many software products that are highly significant for information security are of a commercial nature but are nonetheless given away for free. The purpose of such software may be to strengthen the manufacturer's market position in related markets or to increase its potential customer base for commercial services such as training or

[2816] *See* MARK G. GRAFF & KENNETH R. VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES 55 (2003); MICHEL J.G. VAN EETEN & JOHANNES M. BAUER, OECD, ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES, DSTI/DOC(2008)1, at 42 (2008), *available at* http://www.oecd.org/dataoecd/53/17/40722462.pdf.

[2817] In addition to money, this may include intellectual property rights or the permission to use the consumer's personal information.

consulting.[2818] As discussed *supra* in chapter 5.3.6.1, important examples include Adobe Flash Player, Adobe Reader, and Apple QuickTime.

To also cover free commercial software, it is proposed that they too be subject to the statutory manufacturer warranty. However, since there is no price that consumers could request to be reduced in this scenario, an alternative mechanism is needed to enforce the statutory warranty as applied to free commercial software.

For this purpose, a breach of warranty for a free commercial software (in particular a failure to provide security updates within a reasonable time) should be treated as an unfair business practice[2819] subject to (1) injunctions by competitors, consumer groups, and public authorities as well as (2) penalties to be assessed by a public authority.[2820]

9.2.2. Product Liability in Case of Material Damage

As noted above, software vulnerabilities rarely cause damages that are recoverable under the product liability regimes provided by U.S. or EU law.[2821] However, as regards those few cases, there is no reason why commercial off-the-shelf software should not also be considered a "product."

[2818] *Cf.* HENRY CHESBROUGH, OPEN BUSINESS MODELS: HOW TO THRIVE IN THE NEW INNOVATION LANDSCAPE 45 (2006); ERIC S. RAYMOND, THE CATHEDRAL & THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY 134 et seq. (2001).

[2819] *Cf. supra* chapter 4.1.6 (discussing FTC Act § 5 which prohibits "unfair or deceptive acts or practices") and chapter 6.4.3 (discussing Unfair Commercial Practices Directive art. 5(1) which prohibits "unfair commercial practices").

[2820] Note that this constitutes an indirect risk mitigation measure, not a risk transfer.

[2821] *Cf. supra* chapter 5.3.1 (discussing product liability under U.S. law) and chapter 5.3.3.5 (discussing the types of damages recoverable under the Product Liability Directive).

Accordingly, it is proposed to extend the definition of the term "product" to commercial off-the-shelf software (also referred to as standard software). Specifically as regards the EU's Product Liability Directive, it is further proposed to eliminate the deductible of €500 for property damages.[2822]

In addition to the statutory warranty proposed in the previous chapter, the application of traditional product liability law to software products would further help to align risk and risk mitigation capability as regards software manufacturers and software users.

9.2.3. Excursion: The Necessity of a Means of Collective Redress for Effectuating Direct Risk Transfers

The statutory manufacturer warranty for vulnerability-free software proposed *supra* in chapter 9.2.1 would give many consumers the right to claim rather small amounts of money should the software manufacturer fail to provide patches for publicly reported vulnerabilities. In such a situation, where the risks of litigation—as compared to the potential award—are too large for any single consumer, a means of collective consumer redress is needed to effectuate any risk transfer.

The same applies to the direct risk transfers to be effectuated by the product liability regime proposed *supra* in chapter 9.2.2 and the implied warranty regimes for communications service providers and online service providers proposed *infra* in chapters 9.3.2 and 9.4.2. The availability of a means of collective consumer redress therefore constitutes an integral component of the holistic web of balanced measures proposed here.

[2822] *Cf. supra* chapter 5.3.3.5 (discussing the recoverable damages under Product Liability Directive art. 9(b)). *Cf. also Third Commission report on the application of Council Directive 85/374/EEC*, at 8, COM (2006) 496 final (Sept. 14, 2006) (stating that the €500 deductible is a point of concern since some ask for clarifications while others for its abolition).

While U.S. law provides such a means of collective redress in the form of class actions, EU law currently does not.[2823] In 2007, the European Commission initiated a policy discussion about whether to introduce some form of collective consumer redress[2824] which, however, has not yet resulted in a concrete legislative proposal.

To lend effectiveness to direct risk transfer measures, the EU should adopt a strong system of collective consumer redress and should in particular consider the introduction of an opt-out (rather than opt-in) system for the areas of product liability, manufacturer warranties, and warranties for automated services such as communications services and online services.

9.2.4. Adoption of a Common Risk-Based Software Security Metric

The level of information security provided by any software product is notoriously difficult to assess for users. This not only results in uninformed risk decisions about which software to use[2825] but also helps software manufacturers to minimize the risk of loosing market share due to bad software security, thereby preserving a misalignment between risk and risk mitigation capability.[2826]

An indirect risk transfer should therefore be performed by implementing a targeted transparency policy[2827] that establishes a common risk-based security metric for software

[2823] *See supra* chapter 5.1.7.4.

[2824] *See Commission Green Paper on Consumer Collective Redress*, COM (2008) 794 final (Nov. 27, 2008). *Cf. also* EUROPEAN COMM'N, CONSULTATION PAPER FOR DISCUSSION ON THE FOLLOW-UP TO THE GREEN PAPER ON CONSUMER COLLECTIVE REDRESS (2009), *available at* http://ec.europa.eu/consumers/redress_cons/docs/consultation_paper2009.pdf.

[2825] *Cf. supra* chapter 2.4.3 (discussing the fundamental challenge of uninformed risk decisions).

[2826] *Cf. supra* chapter 2.4.4.

[2827] *Cf. supra* chapter 3.2.3.2 (discussing how targeted transparency policies might effectuate indirect risk transfers).

products. Due to the difficulty of testing the security properties of software,[2828] it is largely recognized that a practical metric for software security has to be based on the vulnerabilities publicly reported after a software has been released.[2829] However, no agreement exists within the software industry as to which vulnerability-based metric should be used.[2830]

It is sometimes also argued that any vulnerability-based metric would make popular software appear less "secure" than it actually is because hackers and vulnerability researchers would primarily focus their efforts on widely deployed software products, thereby reporting a disproportional amount of vulnerabilities in such products. However, this critique implies a conception of "security" that is not risk-based or, at least, does not take the "threat" and "threat agent" risk components into account.[2831] Employing a risk-based conception of information security, it becomes clear that using an unpopular software product which contains 1,000 security vulnerabilities none of which are being discovered is associated with significantly less risk than using a software product which contains 100 vulnerabilities with one being discovered every month.

[2828] *Cf. supra* chapter 4.5.4.2 (discussing the difficulties of product certifications under the Common Criteria); ANDREW JAQUITH, SECURITY METRICS: REPLACING FEAR, UNCERTAINTY, AND DOUBT 83 et seq. (2007) (describing the current state of code security metrics).

[2829] *Cf., e.g.,* ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 54 (2008); Ju An Wang et al., *Security Metrics for Software Systems*, 47 ACM SOUTHEAST REGIONAL CONF. (2009); DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE 88 (2008) (explaining that vulnerabilities are used for software security metrics because "it is all we have" while at the same time heavily criticizing the reliance on the *number* of vulnerabilities as an indicator for software security).

[2830] For example, in 2007, Microsoft published a report comparing Internet Explorer and Firefox on the basis of a vulnerability count. *See* JEFFREY R. JONES, MICROSOFT. INC., BROWSER VULNERABILITY ANALYSIS OF INTERNET EXPLORER AND FIREFOX 11 (2007), *available at* http://blogs.technet.com/cfs-file.ashx/__key/CommunityServer-Components-PostAttachments/00-02-59-48-22/ie_2D00_firefox_2D00_vuln_2D00_analysis.pdf (concluding that "contrary to popular belief, Internet Explorer has experienced fewer vulnerabilities than Firefox"). In repose, Mozilla criticized Microsoft's approach, noting that "counting bugs is less than useful" *See* Mozilla Found., *Critical Vulnerability in Microsoft Metrics*, MOZILLA SECURITY BLOG, Nov. 30, 2007, http://blog.mozilla.com/security/2007/11/30/critical-vulnerability-in-microsoft-metrics/.

[2831] *Cf. supra* chapter 3.1 (discussing the components of any information security risk: asset, safeguard, vulnerability, threat, and threat agent).

While this is counter-intuitive for software developers—after all, a product that only contains 100 instead of 1,000 vulnerabilities is simply thought of as “better”—it directly follows from the fact that there is no risk if there are no threat agents who are capable of mounting a threat and exploiting a vulnerability.

As a case in point, 62 highly severe security vulnerabilities have been reported for the widely used web browser Mozilla Firefox in 2010 while only nine such vulnerabilities were reported during the same time for the considerably less popular browser Opera.[2832] Does that mean that Opera contains fewer vulnerabilities than Firefox? Of course not; however it suggests that using Opera instead of Firefox reduces one’s information security risks.

Even more important than the number of vulnerabilities is a measure of the time span between a vulnerability being publicly reported and the vulnerability being closed by the installation of a security patch. The collective size of such “windows of vulnerability”[2833] very well expresses the level of information security provided by a particular software product.

For example, in 2006, 45 highly severe security vulnerabilities were publicly reported for Mozilla Firefox while only 35 were reported for Microsoft Internet Explorer.[2834] An examination of the time the manufacturers needed to fix reported vulnerabilities reveals that users of Internet Explorer were exposed to a “window of vulnerability” of 284 days while

[2832] This information can be obtained using the National Vulnerability Database’s advanced search functionality. *See* http://web.nvd.nist.gov/view/vuln/search-advanced?cid=9 (last accessed Feb. 10, 2011).

[2833] *Cf.* William A. Arbaugh et al., *Windows of Vulnerability: A Case Study Analysis*, COMPUTER, Dec. 2000, at 52, *available at* http://www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf.

[2834] This information can be obtained using the National Vulnerability Database’s advanced search functionality. *See* http://web.nvd.nist.gov/view/vuln/search-advanced?cid=9 (last accessed Feb. 10, 2011).

users of Firefox only had to browse the web with unpatched critical vulnerabilities for nine days.[2835]

For the sake of simplicity, it was assumed in the above example that users would immediately install patches once they become available. That is, however, typically not the case.[2836] To measure (i.e. to reduce uncertainty about)[2837] when a security patch is installed by users, two factors should be used: (1) the date the patch has been made publicly available and (2) whether the software implements an automatic update feature which is enabled by default.

In summary, a risk-based security metric for software products should be based on the "windows of vulnerability" of a software product, whereas each "window of vulnerability" should be expressed in terms of its size and the severity of the vulnerability as calculated using a common standard such as the Common Vulnerability Scoring System (CVSS).[2838] To users, the metric should be expressed as a simple grade (e.g. one to five or one to ten), possibly supported by color codes.[2839] If a security metric is also adopted for personal information controllers, as proposed *supra* in chapter 9.1.2, the same scheme should be

[2835] *See* Brian Krebs, *Internet Explorer Unsafe for 284 Days in 2006*, WASH. POST, Jan. 4, 2007, http://blog.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html.

[2836] *Cf.* ROSS ANDERSON ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET 64 (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport (noting that "the view among security professionals is that patches are available for the majority of exploits used by attackers").

[2837] *See* DOUGLAS W. HUBBARD, HOW TO MEASURE ANYTHING: FINDING THE VALUE OF INTANGIBLES IN BUSINESS 23 (2010). *Cf. also supra* chapter 4.1.10.4 (briefly discussing the concept of measurement).

[2838] *Cf.* Brian Krebs, *Blogfight: IE Vs. Firefox Security*, WASH. POST, Jan. 29, 2009, http://voices.washingtonpost.com/securityfix/2009/01/blogfight_the_truth_about_ie_v.html (discussing the importance of also considering the severity of vulnerabilities).

[2839] *Cf. also* Parliament and Council Directive 2010/30, art. 10(4)(d), 2010 O.J. (L 153) 1, 7 (EU) (mandating the use of a color scale to inform end-users about products' consumption of energy whereas the color scale "shall consist of no more than seven different colours from dark green to red").

applied. This would not only prevent user confusion but would indeed mutually reinforce the relevance of both metrics.

The information needed to calculate the metric described above is indeed already publicly available.[2840] A regulatory measure aiming to provide targeted transparency would therefore only have to concentrate on two aspects: First, mathematically defining the risk-based metric discussed above. In this regard, a non-regulatory agency such as the National Institute of Standards and Technology (NIST) in the U.S. or the European Network and Information Security Agency (ENISA) in the EU might provide valuable support. Second, mandating that all manufacturers of commercial off-the-shelf software display a software product's security rating before a user orders, buys, or licenses the product (e.g. right above the "download" button on the manufacturer's website).

In conclusion, this targeted transparency regime would facilitate more informed risk decisions by users and would perform an indirect risk transfer to software manufacturers.

9.3. Communications Service Providers

To reduce the misalignment between risk and risk mitigation capability as regards communications service providers and their users, risk should be transferred to providers indirectly by requiring the public disclosure of network security breaches (see *infra* chapter 9.3.1) as well as directly by establishing an implied warranty regime (see *infra* chapter 9.3.2). Furthermore, risk mitigation should be performed by mandating the implementation of "appropriate" safeguards while specifying a risk assessment method by which to determine appropriateness (see *infra* chapter 9.3.3).

[2840] *See* http://nvd.nist.gov (last accessed Feb. 10, 2011).

To the extent that communications service providers act as personal information controllers, they should also be subject to the regulatory requirement of implementing “appropriate” safeguards to protect personal information (see *supra* chapter 9.1.1) as well as to mandatory data security breach notification (see *supra* chapter 9.1.2).

9.3.1. Mandatory Network Security Breach Notification to the Public

Currently, subscribers of communications services (in particular Internet access services) are forced to make uninformed risk decisions when choosing a particular service since there is little public information about the level of availability provided by different service providers. Both EU and U.S. law only require the disclosure of relevant information to public authorities but not to (potential) subscribers.[2841]

This ultimately results in a misalignment between risk and risk mitigation capability because communications service providers do not have to bear the risk of a loss of market share should they provide less availability than their competitors. The mandatory *public* notification of losses of availability (referred in this context as *network security breaches*) could help to better align risk and risk mitigation capability by establishing targeted transparency.[2842] This policy proposal is distinct from data security breach notification[2843] insofar as it focuses on the availability of communications services as opposed to the security of personal information. However, many of the components of both policy proposals are very similar.

The personal scope of application of a network security breach notification policy should cover all types of communications service providers which provide access to a public

[2841] *See supra* chapter 6.3.

[2842] *Cf. supra* chapter 3.2.3.2 (describing the fundamentals of targeted transparency policies).

[2843] *See supra* chapter 9.1.2.

communications network on a commercial basis (in particular Internet access providers and telecommunications operators). An interesting question is whether to also cover those Internet backbone providers which do not simultaneously function as Internet access providers[2844]: Subscribers do not have any direct relation with such providers and can therefore not meaningfully react to a particular network security breach or a generally low level of availability.[2845] Accordingly, network security breach notification is not suitable to perform a risk transfer from subscribers to this group of Internet backbone providers.

However, mandatory network security breach notification for Internet backbone providers may still serve as a risk mitigation measure, specifically a detective measure, which could allow regulators as well as researchers to better assess the current state of global Internet availability.

Accordingly, it is proposed that network security breach notification should be used as an indirect risk transfer measure regarding Internet access providers and as a detective security measure regarding Internet backbone providers.

As already discussed in the context of data security breach notification, a successful targeted transparency policy requires (1) that users perceive the breach information to have value;[2846] (2) that the breach information is compatible with individuals' decision-making processes in

[2844] *Cf. supra* chapter 2.3.1 (discussing the nature of Internet access providers and Internet backbone providers).

[2845] Indeed, subscribers would simply not know how to react to network security breach reports from Internet backbone providers. *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 61 (2007) (arguing that the color-coded terrorism threat advisory levels currently still used the U.S. did not work in particular because it fails to guide individuals' actions meaningfully).

[2846] *Cf.* ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 55 (2007).

particular with regard to the information's format and its time and place of availability;[2847] and (3) that the breach information is easily comprehensible for individuals.[2848]

In order to fulfill the first requirement, short-term outages should not be excluded since many short-term outages can be as significant as a single longer one. All outages should have to be reported but should be weighted by their duration and the number of affected users. This would ensure that users perceive the breach information to have value for furthering their interests (in particular choosing an Internet access provider that offers a sufficient level of availability).

To fulfill the second requirement, it is necessary to establish a central breach repository that allows users to compare the past availability record of a particular provider with that of its competitors before choosing to pay for the provider's services. All notifications should therefore have to be addressed to a central government agency (e.g. the FCC in the U.S. or ENISA in the EU) which could operate the breach repository on a dedicated website. Like the repository proposed for data security breaches, the network security breach repository should make all notices available in easily accessible (e.g. HTML) as well as structured data formats (e.g. XML) and should provide a customizable push technology (e.g. e-mail) so that individuals (e.g. a reporter) can choose to get informed of breaches that meet specific criteria.

Additionally, notifications should also have to be addressed to a provider's subscribers.[2849] Such individual notification should contain, in addition to the information items described

[2847] *Cf. id.* at 56.

[2848] *Cf. id.* at 59.

[2849] This requirement, of course, only applies to communications service providers that have subscribers. In particular that excludes Internet backbone providers which would only have to notify a public authority.

infra, a reference to the website of the central breach repository maintained by the government authority. This ensures that individual notifications will raise awareness for the existence of the central network security breach repository, thereby increasing the information's compatibility with users' decision-making processes. However, since individual notifications are only of subordinate importance, it should be sufficient to have such notifications performed by individual electronic messages or other similarly inexpensive means.

The third requirement of ensuring that the breach information is easily comprehensible for individuals necessitates (1) the prescription of certain information items to be included in any breach notification and (2) that the government agency that maintains the central breach repository develops metrics to better communicate the level of availability provided by a certain communications provider.

Each breach notification should have to contain at least the following information items: (1) date and time of the onset of the outage; (2) duration of the outage; (3) the communications network or service affected; (4) the geographic areas affected; (5) a description of the problem that can be understood by laypersons; (6) a technical description of the problem that allows experts to better understand and learn from the incident; and (7) the number of subscribers as well as the estimated number of affected users.[2850]

Based on these information items, a service availability metric has to be developed that makes it effortless for users to understand the level of availability achieved by a certain provider.

[2850] Note that these numbers can differ significantly because a single subscriber's account can be used by multiple users (e.g. the members of a household or the employees of a corporation).

This metric should be expressed in the same way as the metrics for personal information controllers[2851] and software manufacturers.[2852]

Lastly, to address the challenge of multilingualism in the EU, all breach notifications should be issued in two languages, the official language of the Member State having jurisdiction and English. This replicates the approach chosen for data security breach notifications.[2853]

9.3.2. Implied Warranties for Services

As discussed *supra* in chapter 5.2.2, neither U.S. law nor EU law impose limitations on warranty disclaimers by Internet access providers. This allows them to largely avoid contractual liability for security breaches—in particular for losses of availability.

To better align risk and risk mitigation capability, a warranty regime should be adopted that provides, as a remedy, the right to request a reduction of the price should the service not be in conformity with the service contract. Similar to article 2 of the Consumer Sales Directive, consumers' reasonable expectations should serve as a basis for implied warranties.

While service providers should be able to contractually define the properties of their services, they should not be permitted to generally disclaim implied warranties or eliminate the remedy of a price reduction.

[2851] *See supra* chapter 9.1.2.

[2852] *See supra* chapter 9.2.3.

[2853] *See supra* chapter 9.1.2 (further explaining this pragmatic approach).

9.3.3. Requiring "Appropriate" Safeguards and Defining a Risk Assessment Method to Determine What is "Appropriate"

Currently, only EU law requires communications service providers to implement "appropriate" safeguards to maintain availability of their services.[2854] Given that the availability of communications services is of very high concern for information security in general, U.S. policy makers should consider adopting a similar regulatory risk mitigation measure.

However, requiring "appropriate" safeguards is in itself meaningless, if no guidance is provided as to what is considered "appropriate." Precisely for this reason, the requirements currently existing under EU law are largely ineffective.[2855]

Accordingly, the EU should amend the Telecoms Framework Directive by defining—and the U.S. should adopt a similar measure that includes a definition of—a risk assessment method that allows providers as well as regulators enforcing the requirements to objectively determine whether implemented safeguards are "adequate." Similar to the risk assessment method needed to determine appropriateness with regard to the protection of personal information,[2856] such a method should (1) be quantitative in nature so that it can produce verifiable results; (2) clearly express uncertainty; (3) address the psychological challenges humans face when

[2854] *Cf. supra* chapter 4.3.1 (discussing Telecoms Framework Directive art. 13a(1)).

[2855] *Cf. supra* chapter 4.3.4.1.

[2856] *See supra* chapter 9.1.1.

estimating risks; and (4) provide guidance for how to measure and quantitatively express a risk's potential impact on information security.[2857]

Since the development of such a method is very challenging, policy makers should approach the problem in a three-step process: (1) funding research and standardization efforts; (2) assessing the quality of the emerging risk assessment standards; and (3) mandating the use of a specific standard for enforcement purposes.

The required safeguards should not only address the risk of service unavailability but should also aim to protect an Internet access provider's subscribers from malware, to the extent "appropriate." In particular, appropriate safeguards might encompass measures to mitigate the risks of botnets such as quarantining infected machines[2858] or making it more difficult for compromised computers to be used as spam-relays.[2859]

This regulatory approach, based on requiring "appropriate" safeguards, is to be favored over an approach that requires specific safeguards: If a regulatory authority were empowered to establish specific security requirements for communications service providers, the primary

[2857] The challenges of performing risk assessments are discussed in the context of the security personal information. *See supra* chapter 4.1.10.4.

[2858] *Cf.* ENISA, PROVIDER SECURITY MEASURES PART 1: SECURITY AND ANTI-SPAM MEASURES OF ELECTRONIC COMMUNICATION SERVICE PROVIDERS – SURVEY 4 (2006), *available at* http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures/studies/provider-security-measures-1/at_download/fullReport (stating that 75% of the responding ISPs claimed to quarantine infected PC).

[2859] *Cf. id.* at 7 (stating that 28% of the responding ISPs claimed to reject straight SMTP traffic from consumer connections). RFC 4409 provides that port 25 should only be used for relaying mails from one mail server to another; mail submission (i.e. the process of submitting an e-mail from the sending client to the outgoing mail server), on the other hand, should only be performed on port 587. *See* R. GELLENS & J. KLENSIN, MESSAGE SUBMISSION FOR MAIL, RFC 4409 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4409.txt. If RFC 4409 was implemented by all outgoing mail servers, Internet access providers could block port 25 since subscribers typically do not operate their own mail server at home. *Cf.* Brian Krebs, *Verizon to Implement Spam Blocking Measures*, WASH. POST, Feb. 27, 2009, http://voices.washingtonpost.com/securityfix/2009/02/verizon_to_implement_spam_bloc.html (reporting that Verizon, like many other Internet access providers in the U.S. will start to block port 25).

burden of performing a high-quality risk assessment as well as the burden of selecting appropriate mitigating measures would fall on the government. However, in particular with regard to the selection of appropriate mitigating measures for communications service providers, a government authority would face significant obstacles.

First, measures that would effectively require modifications of the Internet's core protocols (in particular IP and the inter-AS routing protocol BGP)[2860] directly challenge the current form of Internet governance, which is characterized by private-sector leadership.[2861]

Second, due to the complexity of the Internet's logical infrastructure and the interdependencies between different parts of that infrastructure, many problems do not have an easy solution. A government regulator would therefore have to have an extraordinary amount of expertise which, however, regulators typically lack.

Third, many security risks involving the Internet's logical infrastructure are characterized by network effects,[2862] meaning that the effectiveness of a particular safeguard depends on how many other providers across the world are implementing the same safeguard.

[2860] *Cf. supra* chapter 2.3.1.

[2861] *Cf. Commission Communication on Internet governance: the next steps*, at 3, COM (2009) 277 final (June 18, 2009). *Cf. also* WORKING GROUP ON INTERNET GOVERNANCE [WGIG], REPORT OF THE WORKING GROUP ON INTERNET GOVERNANCE 4 (2005), *available at* http://www.wgig.org/docs/WGIGREPORT.pdf (emphasizing the importance of a multi-stakeholder approach by defining "Internet governance" as "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet"); MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 154 et seq. (2002) (describing how the U.S. government somewhat limited the private sector's role but still left it in a leading position as regards Internet governance).

[2862] *Cf.* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 45 (1999) (generally describing network effects); Marc Lelarge & Jean Bolot, *Network Externalities and the Deployment of Security Features and Protocols in the Internet*, 2008 ACM SIGMETRICS 37 (presenting a model to quantify the impact of network effects on the adoptability and deployment of security features and protocols in the Internet).

All three obstacles are demonstrated very well by the example of IP routing risks. As discussed *supra* in chapter 2.3.1, the exchange of routing information between Autonomous Systems (ASes) is performed by an exterior gateway protocol known as the Border Gateway Protocol (BGP).[2863] BGP suffers from intrinsic vulnerabilities as it does not allow for the verification of the integrity and authenticity of routing information communicated between different ASes. Accidents or intentional actions by malicious threat agents can therefore result in a re-routing of global Internet traffic, thereby threatening the confidentiality, integrity, and availability of information.[2864] For example, in May 2003, spammers hijacked a U.S. military contractor's IP address space (referred to as a *prefix*) to send spam;[2865] in May 2004, a Malaysian ISP re-routed all Internet traffic directed at Yahoo's Santa Clara data center to itself;[2866] in December 2004, a Turkish ISP sent out incorrect routing information that resulted in the re-routing of *all* Internet traffic to itself;[2867] in February 2008, Pakistan Telecom—in an attempt to censor YouTube in Pakistan—inadvertently blocked worldwide access to YouTube.com for two hours by sending incorrect routing information to its upstream provider

[2863] Border Gateway Protocol 4 (BGP-4) has become the de-facto standard as an exterior gateway protocol. It is specified in Y. Rekhter et al., A Border Gateway Protocol 4 (BGP-4), RFC 4271 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4271.txt. *Cf.* Ravi Malhotra, IP Routing 157 (2002).

[2864] *Cf.* A. Barbir et al., Generic Threats to Routing Protocols, RFC 4593, at 12 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4593.txt; Tao Wan et al., *A selective introduction to border gateway protocol (BGP) security issues, in* Aspects of Network and Information Security 152, 159 et seq. (Evangelos Kranakis et al. eds., 2008); Daniel Mende et al., ERNW, All Your Packets Are Belong to Us □ Attacking Backbone Technologies 7 (2009), *available at* http://www.ernw.de/content/e7/e181/e1309/download1360/ERNW_White_paper_All_your_packets_ger.pdf. The threats to confidentiality have been discussed in particular by Alex Pilosov and Tony Kapela at the Defcon conference in 2008. *See* http://www.wired.com/images_blogs/threatlevel/files/edited-iphd-2.ppt (last accessed Feb. 10, 2011). *See also* Kim Zetter, *Revealed: The Internet's Biggest Security Hole*, Wired.com, Aug. 26, 2008, http://www.wired.com/threatlevel/2008/08/revealed-the-in/.

[2865] *See* Laris Benkis, Renesys, Practical BGP Security: Architecture, Techniques and Tools 1 (2005), *available at* http://www.renesys.com/tech/notes/WP_BGP_rev6.pdf.

[2866] *See id.* at 12.

[2867] *See* Alin C. Popescu et al., The Anatomy of a Leak: AS9121 or How We Learned to Start Worrying and Hate the Maximum Prefix Limits (May 15, 2005), http://www.nanog.org/meetings/nanog34/presentations/underwood.pdf.

which propagated the false routing information across the Internet;[2868] and in April 2010, China Telecom hijacked a significant portion of the Internet routes for 18 minutes.[2869]

To mitigate this risk, the specification of BGP has to be amended. To do so by regulatory action is very difficult for the reasons mentioned above: The technical standard describing BGP, RFC 4271,[2870] is maintained by the Internet Engineering Task Force (IETF), a private sector entity. Interfering with the current "rough consensus"-based standardization approach[2871] by imposing specific amendments would severely upset the current process of innovation as regards the Internet's core protocols.[2872]

Furthermore, amending the BGP standard in a way that it provides integrity and authenticity of all routing information communicated between different ASes is indeed a highly challenging task. To provide integrity and authenticity, asymmetric cryptographic signatures will have to be used and a secure key exchange mechanism will have to be defined. Solutions proposed so far include the U.S. government-funded Secure Border Gateway Protocol

[2868] *See* RIPE NCC, YouTube Hijacking: A RIPE NCC RIS case study (Feb. 28, 2008), http://www.ripe.net/news/study-youtube-hijacking.html. *See also* Carolyn Duffy Marsan, *Six worst Internet routing attacks*, NETWORK WORLD, Jan. 15, 2009, http://www.networkworld.com/news/2009/011509-bgp-attacks.html.

[2869] BGPmon, *Chinese BGP hijack, putting things into perspective*, BGPMON BLOG, Nov. 21, 2010, http://bgpmon.net/blog/?p=323; U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2010 REPORT TO CONGRESS 243 (2010), *available at* http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf.

[2870] Y. REKHTER ET AL., A BORDER GATEWAY PROTOCOL 4 (BGP-4), RFC 4271 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4271.txt.

[2871] *See* S. BRADNER, IETF WORKING GROUP GUIDELINES AND PROCEDURES, RFC 2418, at 12 (1998), ftp://ftp.rfc-editor.org/in-notes/rfc2418.txt ("Working groups make decisions through a 'rough consensus' process. IETF consensus does not require that all participants agree although this is, of course, preferred. In general, the dominant view of the working group shall prevail. […] Note that 51% of the working group does not qualify as 'rough consensus' and 99% is better than rough. It is up to the Chair to determine if rough consensus has been reached.").

[2872] While not directly related to information security, the role the Internet's core protocols play for innovation must not be underestimated. *See generally* BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION (2010).

(S-BGP),[2873] the AT&T-supported Interdomain Route Validation (IRV),[2874] the Cisco-developed and U.S. government-funded Extensions to BGP to Support Secure Origin BGP (soBGP),[2875] and Pretty Secure BGP (psBGP).[2876] Most recently, the IETF's Secure Inter-Domain Routing Working Group has started to draft proposals for a Resource Public Key Infrastructure (RPKI)[2877] which could support yet another more secure version of BGP, termed BGPsec.[2878] To make a sound decision as to which draft standard should be implemented, let alone to develop such a standard on its own, is typically beyond the capabilities of a regulatory authority. In this regard, the eSignature Directive serves as a warning example.[2879]

Lastly, the network effects inherent to inter-AS routing necessitate wide-ranging adoption if any of the proposed solutions are to work in practice. For example, if the EU unilaterally

[2873] *See* Stephen Kent et al., *Secure Border Gateway Protocol (S-BGP)*, 18 IEEE J. ON SELECTED AREAS IN COMM. 582 (2000).

[2874] *See* Geoffrey Goodell et al., *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing*, *in* 2003 NETWORK AND DISTRIBUTED SYSTEMS SECURITY 75, *available at* http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/5.pdf.

[2875] Russ White, Cisco Systems, *Securing BGP Through Secure Origin BGP*, INTERNET PROTOCOL J., Sept. 2003, at 15, *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/ipj_6-3.pdf; James Ng, Cisco Systems, Extensions to BGP to Support Secure Origin BGP (soBGP) (Apr. 2004), http://tools.ietf.org/html/draft-ng-sobgp-bgp-extensions-02.

[2876] P. C. van Oorschot et al., *On interdomain routing security and pretty secure BGP (psBGP)*, ACM TRANSACTIONS ON INFO. AND SYSTEM SECURITY, July 2007, *available at* http://delivery.acm.org/10.1145/1270000/1266980/a11-oorschot.pdf?key1=1266980&key2=2309656921&coll=DL&dl=ACM&CFID=7524552&CFTOKEN=54618690.

[2877] The working group's documents are available at http://tools.ietf.org/wg/sidr/ (last accessed Feb. 10, 2011). Note that a RPKI could give unprecedented operational authority to IANA and the Regional Internet Registries (*cf. supra* chapter 2.3.1) since they might be capable of effectively invalidating route information for particular IP address ranges by revoking an AS's certificate.

[2878] *See* S. Bellovin et al., Security Requirements for BGP Path Validation (Jan. 29, 2011), http://tools.ietf.org/html/draft-ymbk-bgpsec-reqs-00 (stating that "[t]his document describes requirements to be placed on a future BGP security protocol, herein termed BGPsec").

[2879] *Cf. supra* chapters 4.3.3 and 4.5.3 (discussing a number of major deficiencies of the EU's regulation of electronic signatures).

required all Internet access providers and Internet backbone providers in the EU to implement a particular security solution for inter-AS routing, the EU's providers would still be vulnerable to the hijacking of address ranges belonging to ASes in the U.S.

In summary, regulatory authorities are not in a good position to impose specific security requirements on communications service providers. Regulatory policies should therefore be limited to requiring "adequate" safeguards whereas "adequacy" would have to be determined in accordance with a specified quantitative risk assessment method. Additionally, non-regulatory measures—which are outside the scope of this thesis—like funding of relevant research should also be considered.

9.4. Providers of Online Services

Online service providers that store, process, or transmit personal information should be subject to the same regulatory measures as all other personal information controllers (see *infra* chapter 9.4.1). Furthermore, they should also be subjected to an implied warranties regime (see *infra* chapter 9.4.2).

9.4.1. Regulatory Requirements as Personal Information Controllers

To the extent that online service providers act as personal information controllers, they should be subject to the regulatory requirement of implementing "appropriate" safeguards to protect personal information (see *supra* chapter 9.1.1) as well as to mandatory data security breach notification (see *supra* chapter 9.1.2).

As argued above, data security breach notification should also cover breaches of information availability if the personal information was maintained for the benefit of the individual. In this regard, data security breach notification fulfills a similar role for online service providers as does network security breach notification for communications service providers.

9.4.2. Implied Warranties for Services

The same warranty regime that is proposed *supra* for communications service providers[2880] should apply equally to online service providers, making implied warranties binding on online service providers and providing, as a remedy, the right to request a reduction of the price should the service not be in conformity with the service contract. At least as regards commercial online services and their users, this will help to better align risk and risk mitigation capability.[2881]

9.5. Malicious Actors

The "threat agent" risk component can be addressed by deterring malicious threat agents from mounting any information security threats. As discussed *supra* in chapter 7.4.1 , such deterrence is, however, limited since the attribution problem inherent to the Internet results in a very low certainty of punishment.

Nonetheless, it is proposed *infra* to at least criminalize one particular type of malicious activity that has become the most threatening phenomenon in the cybercrime landscape: botnet activity.[2882]

[2880] *See supra* chapter 9.3.2.

[2881] A question that is beyond the scope of this policy proposal and should be the subject of further research is how to value copyright licenses and rights to personal information users grant providers in exchange for their services. *Cf. supra* chapter 5.2.2 (briefly pointing out that many online services are claimed to be provided "for free" when indeed they are not: users have to grant the provider rights to uploaded content in order to be allowed to use the service).

[2882] *Cf. also supra* chapter 7.4.2 (discussing the difficulties of applying U.S. and EU computer crime law to botnets).

9.5.1. Criminalizing Botnet Activity

The Computer Fraud and Abuse Act (hereinafter *CFAA*),[2883] and article 2 of the EU's Framework Decision on Attacks Against Information Systems (hereinafter *Framework Decision*)[2884] should be amended to clarify that gaining unauthorized access to a large number of computers constitutes a criminal offense even if the attacker does not (and has not intent to) alter, obtain, or delete any information stored on the computers.[2885] This would eliminate the defense of "only" having built a botnet with the intent to send spam, perpetrate click fraud, perform a distributed denial of service (DDoS) attack, or sell the botnet to the highest bidder.

Many computers are compromised (and subsequently joined into a botnet) not by exploiting a technical vulnerability but by performing social engineering (e.g. tricking users into installing a Trojan horse). Accordingly, CFAA, California Penal Code § 502(c),[2886] New York Penal Law § 156.05,[2887] and Framework Decision article 2 should be amended to clarify that compromising a large number of computers constitutes a criminal offense, irrespective of how the computers are compromised.

9.6. Governments Authorities

Government authorities often perform the role of personal information controllers. As such they should be subject to the same regulatory measures as all other personal information

[2883] *Cf. supra* chapter 7.1.1.

[2884] *Cf. supra* chapter 7.3.

[2885] CAL. PENAL CODE § 502(c) and N.Y. PENAL LAW § 156.05 already cover any unauthorized access to a computer, irrespective of whether the attacker acts with the intent to alter, obtain, or delete any information. *See supra* chapters 7.2.1 and 7.2.2.

[2886] *Cf. supra* chapter 7.2.1.

[2887] *Cf. supra* chapter 7.2.2.

controllers (see *infra* chapter 9.6.1). Furthermore, they should also be required to implement appropriate safeguards for non-personal information (see *infra* chapter 9.6.2).

9.6.1. Regulatory Requirements as Personal Information Controllers

Like communications service providers[2888] and online service providers,[2889] government authorities should be subject to the regulatory requirement of implementing "appropriate" safeguards to protect personal information (see *supra* chapter 9.1.1) as well as to mandatory data security breach notification (see *supra* chapter 9.1.2) to the extent that they act as personal information controllers.

With regard to data security breach notification it has to be noted that the risk government authorities would face due to low levels of information security would obviously not be of an economic but a political nature. This nonetheless constitutes an important risk transfer that will help to better align risk and risk mitigation capability as regards government authorities and the individuals concerned.

9.6.2. Mandatory "Appropriate" Safeguards for Non-Personal Information

Government authorities also store, process, and transmit vast amounts of non-personal information. To mitigate risks to that information, government authorities should be required to implement appropriate safeguards. U.S. federal law, in the form of the Federal Information

[2888] *See supra* chapter 9.3.

[2889] *See supra* chapter 9.4.1.

Security Management Act of 2002 (hereinafter *FISMA*), does so[2890] while EU law generally does not.[2891]

The risk management standard adopted pursuant to FISMA advocates the use of a qualitative scoring method[2892] which necessarily suffers from range compression, unnecessary ambiguity, and a general lack of objective and verifiable results.[2893] Furthermore, the metrics used so far to monitor compliance, have focused more on the extent to which the documentation of an agency's policies, procedures, and practices complied with FISMA than on the extent of compliance of actual procedures and practices. Whether the new metrics introduced in April 2010[2894] will bring significant change still remains to be seen. In any case, FISMA should be amended to require federal agencies to use a specific risk assessment method that should (1) be quantitative in nature so that it can produce verifiable results; (2) clearly express uncertainty; (3) address the psychological challenges humans face when estimating risks; and (4) provide guidance for how to quantitatively measure a risk's potential impact on information.

The EU should consider adopting similar regulatory measures for EU institutions and their agencies. Since the EU currently has no competence that would allow it to prescribe such

[2890] *See supra* chapter 4.4.1.

[2891] The Commission's and the Council's Rules of Procedure only require the protection of classified information. *See supra* chapter 4.4.2.

[2892] *See* NIST, RISK MANAGEMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS, SPECIAL PUBLICATION 800-30, at 25 (2002), *available at* http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[2893] *Cf.* DOUGLAS W. HUBBARD, THE FAILURE OF RISK MANAGEMENT: WHY IT'S BROKEN AND HOW TO FIX IT 73 (2009) (specifically criticizing NIST's Special Publication 800-30 for its use of ineffective risk assessment methods). *Cf. also supra* chapter 4.1.10.4 (discussing the shortcomings of scoring methods).

[2894] OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-10-15, FY 2010 REPORTING INSTRUCTIONS FOR THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT AND AGENCY PRIVACY MANAGEMENT (2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

requirements for Member State governments,[2895] it should at least provide guidance to Member States in this area.

[2895] Article 16 of the Treaty on the Functioning of the European Union as amended by Treaty of Lisbon provides the EU with a broad competence in the area of the protection of personal data (*cf. supra* chapter 2.2.1). However, the EU has no competence in the area of the protection of non-personal data. *Cf.* art. 5 of the Treaty on European Union as amended by the Lisbon Treaty (re-iterating the principle of conferral of competences).

10. Conclusion

Today's "information society" is becoming more and more dependent on the confidentiality, integrity, and availability of information. This applies to personal information as well as non-personal information (e.g. corporate financial information subject to mandatory reporting).

In recognition of the importance of information security, U.S. law as well as EU law increasingly dedicates regulatory attention to different actors of the information security landscape: providers of communications services, providers of online services, software manufacturers, other businesses—in particular in their capacity as personal information controllers—consumers, governments, and malicious actors. Chapters 4 to 7 have analyzed the numerous regulatory policies adopted in the U.S. and EU addressing information security. These chapters therefore provide a unique comparative analysis of information security law in the EU and the U.S. as it stands today. As regards the U.S., the following laws have been discussed: the Children's Online Privacy Protection Act, the Communications Act, the Communications Decency Act, the Computer Fraud and Abuse Act, the Department of Veterans Affairs Information Security Enhancement Act, the Electronic Fund Transfer Act, the Fair Credit Reporting Act, the Federal Food, Drug, and Cosmetic Act, the Federal Information Security Management Act, the Federal Trade Commission Act, the Gramm-Leach-Bliley Act, the Health Information Technology for Economic and Clinical Health Act (HITECH Act), the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act, the Stored Communications Act, the Truth in Lending Act, the Wiretap Act, the NERC Standards, OMB Memorandum M-07-16, and various California and New York state laws such as California Assembly Bills 1950 and 1386, and the New York Information Security Breach and Notification Act as well as the common law of strict tort liability and the common law of negligence. The analysis of information security law in the EU covered in particular the Consumer Sales Directive, the Data Protection Directive, the E-Commerce Directive, the ePrivacy Directive, the eSignature Directive, the Fourth Company Law Directive, the Framework Decision on Attacks Against Information Systems, the Medical Devices Directive, the Payment Services Directive, the Product Liability Directive, the Statutory Audit Directive, the Telecoms Framework Directive, and the Unfair Commercial Practices Directive.

In order to comparatively assess these regulatory measures, a risk-based assessment methodology has been developed in chapter 3. On a fundamental level, this methodology is intended to support rational, risk-based assessments of currently enacted regulatory policies as well as any future policy proposals, thereby helping to actually increase information security rather than engage in "security theatre." This methodology provides a differentiation between the risk treatment options of risk mitigation, risk avoidance, risk transfer, and risk acceptance. It thereby establishes a theoretical structure for the entire policy area of information security and, more importantly, allows for a better understanding of how regulatory policies affect information security risks.

Building on the analysis of individual regulatory policies in chapters 4 to 7, an overall comparative assessment was provided in chapter 8. This assessment revealed that risk mitigation is the risk treatment option implemented by an overwhelming majority of regulatory policies while risk transfer measures are rather few and comparatively weak. Information security law in the EU and the U.S., as it stands today, also fails to adequately address any of the fundamental challenges in the area of information security: (1) the imperfection of technology; (2) the imperfection of people; (3) uninformed risk decisions and the difficulty of measuring security; and (4) the misalignment between risk and risk mitigation capability. Lastly, it was shown that the information security law of both jurisdictions does not regulate the most important type of actors of the information security landscape evenly. U.S. information security law regulates personal information controllers more than any other type of actor while EU information security law regulates communications service providers the most. Significantly, neither the U.S. nor the EU provides regulatory measures addressed at software manufacturers.

Drawing from these observations, chapter 9 presented a holistic policy proposal for how to fundamentally improve the current state of information security in the EU and the U.S. The proposal would dedicate regulatory attention evenly to personal information controllers, software manufacturers, communications service providers, online service providers, malicious actors as well as government authorities. In doing so, it would adopt a rather novel approach to information security regulation by assigning central importance to regulatory measures that would perform indirect risk transfers by establishing targeted transparency.

By presenting a holistic policy proposal as well as a risk-based methodology for assessing regulatory information security policies, this thesis will hopefully advance policy discussions in the U.S. and the EU and will ultimately help policy makers to implement more effective policy solutions that have the potential to fundamentally improve information security.

Bibliography

ABA SECTION OF ANTITRUST LAW, STATE ANTITRUST PRACTICE AND STATUTES (3d ed. 2004)

Abbamonte, Giuseppe B., *The Unfair Commercial Practices Directive: An Example of the New European Consumer Protection Approach*, 12 COLUM. J. EUR. L. 695 (2006)

Achenbach, Joel & Fahrenthold, David A., *Oil spill dumped 4.9 million barrels into Gulf of Mexico, latest measure shows*, WASH. POST, Aug. 3, 2010, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080204695_pf.html

Achenbach, Joel & Fahrenthold, David, *Oil-spill flow rate estimate surges to 35,000 to 60,000 barrels a day*, WASH. POST, June 15, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/06/15/AR2010061504267_pf.html

Acquisti, Alessandro & Grossklags, Jens, *Privacy Attitudes and Privacy Behavior, in* ECONOMICS OF INFORMATION SECURITY 165 (L. Jean Camp & Stephen Lewis eds., 2004)

ACRET, JAMES, CONSTRUCTION LITIGATION HANDBOOK (2d ed. 2010)

ADAMS, CARLISLE & LLOYD, STEVE, UNDERSTANDING PKI: CONCEPTS, STANDARDS, AND DEPLOYMENT CONSIDERATIONS (2d ed. 2003)

Aguilar, Luis A., Statement of Commissioner Luis A. Aguilar Regarding His Commitment to Implementation of Sarbanes-Oxley Section 404(b) (Oct. 2, 2009) (transcript available at http://www.sec.gov/news/speech/2009/spch100209laa.htm)

Akerlof, George A., *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. OF ECON. 488 (1970)

Albanese, Ferdinando, *Legal Harmonisation in Europe, Product Liability: A Comparison Between the Directive of the European Communities and the Council of Europe Convention*, *in* COMPARATIVE PRODUCT LIABILITY 15 (C. J. Miller ed., 1986)

Alces, Peter A. & Book, Aaron S., *When Y2K Causes "Economic Loss" to "Other Property"*, 84 MINN. L. REV. 1 (1999)

Aleph1, *Smashing The Stack For Fun And Profit*, PHRACK, Nov. 8, 1996, http://www.phrack.org/issues.html?issue=49&id=14#article

Allen, Rosalind K., *Tough New FCC Rules on Customer Call Records*, COMM. LAW., Spring 2007, at 32

AM. BAR ASS'N, DATA SECURITY HANDBOOK (2008)

AM. L. INST., PRINCIPLES OF THE LAW OF SOFTWARE CONTRACTS, TENTATIVE DRAFT NO. 1 (2008)

Amant, Brendan St., *The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 HARV. J. ON LEGIS. 505 (2007)

Ambrose, Stephen F. & Gelb, Joseph W., *Consumer Privacy Regulation, Enforcement, and Litigation in the United States*, 58 BUS. LAW. 1181 (2003)

Ammon, Ulrich, *Language conflicts in the European Union*, 16 INT'L J. OF APPLIED LINGUISTICS 319 (2006)

ANAND, SANJAY, SARBANES-OXLEY GUIDE FOR FINANCE AND INFORMATION TECHNOLOGY PROFESSIONALS (2006)

ANDERLE, CHRISTOPH, DER HAFTUNGSUMFANG DES HARMONISIERTEN PRODUKTHAFTUNGSRECHTES [THE EXTENT OF LIABILITY UNDER HARMONIZED PRODUCT LIABILITY LAW] (1990)

Anderson, Ross & Moore, Tyler, *Information Security Economics – and Beyond*, 27 ANN. INT'L CRYPTOLOGY CONF. 68 (2007), *available at* http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf

Anderson, Ross & Moore, Tyler, *The Economics of Information Security*, 314 SCIENCE 610 (2006)

ANDERSON, ROSS ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET (2008), *available at* http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport

ANDERSON, ROSS J., SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS (2d ed. 2008)

Anderson, Ross, *Why Information Security is Hard – An Economic Perspective*, 17 ANN. COMPUTER SECURITY APPLICATIONS CONF. 358 (2001)

ANDRESEN, KATHERYN A., 1 LAW AND BUSINESS OF COMPUTER SOFTWARE (2d ed. 2009)

Arbaugh, William A. et al., *Windows of Vulnerability: A Case Study Analysis*, COMPUTER, Dec. 2000, at 52, *available at* http://www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf

Ardia, David S., *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373 (2010)

Arkin, Sharon J., *The Unfair Competition Law after Proposition 64: Changing the Consumer Protection Landscape*, 32 W. ST. U. L. REV. 155 (2005)

Arledge, Christopher W., *Standing Under the Unfair Competition Law is Unlikely to Exist for Competitors*, 50 ORANGE COUNTY LAW. 51 (2008)

Arnet, George W., III, *The Death of Glass-Steagall and the Birth of the Modern Financial Services Corporation*, 203 N.J. LAW. 42 (2000)

Arnold, Paul P., *Give Smaller Companies A Choice: Solving Sarbanes-Oxley Section 404 Inefficiency*, 42 U. MICH. J.L. REFORM 931 (2009)

Avery, Robert B. et al., *An Overview of Consumer Data and Credit Reporting*, FED. RES. BULL. (Board of Governors of the Federal Reserve System, Washington, D.C.), Feb. 2003, at 47, *available at* http://www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf

Axelsson, Stefan, *The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection*, 1999 ACM CONFERENCE ON COMPUTER AND COMMC'NS SECURITY 1

Backer, Larry Cata, *Surveillance and Control: Privatizing and Nationalizing Corporate Monitoring After Sarbanes-Oxley*, 2004 MICH. ST. L. REV. 327

Bain, Ben, *Improved FISMA scores don't add up to better security, auditor says*, FEDERAL COMPUTER WEEK, June 29, 2009

BAINBRIDGE, DAVID, EC DATA PROTECTION DIRECTIVE (1996)

Baistrocchi, Pablo Asbo, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 111 (2002)

BAKER, WADE, VERIZON, 2010 DATA BREACH INVESTIGATIONS REPORT (2010), *available at* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

BARBIR, A. ET AL., GENERIC THREATS TO ROUTING PROTOCOLS, RFC 4593 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4593.txt

Barnes, Douglas A., Note, *Deworming the Internet,* 83 TEX. L. REV. 279 (2004)

Barron, Cheryll Aimée, *High tech's missionaries of sloppiness*, SALON.COM, Dec. 6, 2000, http://www.salon.com/technology/feature/2000/12/06/bad_computers

Baset, Salman A. & Schulzrinne, Henning, *An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol,* 25 IEEE INT'L CONF. ON COMPUTER COMM. 2695 (2006)

BASS, LEWIS, PRODUCTS LIABILITY: DESIGN AND MANUFACTURING DEFECTS (2d ed. 2009)

Bauer, Axel, *Produkthaftung für Software nach geltendem und künftigem deutschen Recht* [*Product Liability for Software Under Current and Future German Law*], 1989 PRODUKTHAFTPFLICHT INTERNATIONAL 39 (F.R.G.)

Bauer, Axel, *Produkthaftung für Software nach geltendem und künftigem deutschen Recht (Teil 2)* [*Product Liability for Software Under Current and Future German Law (Part 2)*], 1989 PRODUKTHAFTPFLICHT INTERNATIONAL 98 (F.R.G.)

Bauer, Johannes M. & van Eeten, Michel J.G., *Cybersecurity: Stakeholde rincentives, externalities, and policy options*, 33 TELECOMM. POL'Y 706 (2009)

BECCARIA, CESARE, AN ESSAY ON CRIMES AND PUNISHMENTS 62 (Adolph Caso trans., 2008) (1764)

Bejtlich, Richard, *Thoughts on New OMB FISMA Memo*, TAOSECURITY, Apr. 24, 2010, http://taosecurity.blogspot.com/2010/04/thoughts-on-new-omb-fisma-memo.html

Bellovin, S. et al., Security Requirements for BGP Path Validation (Jan. 29, 2011), http://tools.ietf.org/html/draft-ymbk-bgpsec-reqs-00

BENKIS, LARIS, RENESYS, PRACTICAL BGP SECURITY: ARCHITECTURE, TECHNIQUES AND TOOLS (2005), *available at* http://www.renesys.com/tech/notes/WP_BGP_rev6.pdf

BENKLER, YOCHAI, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006)

BGPmon, *Chinese BGP hijack, putting things into perspective*, BGPMON BLOG, Nov. 21, 2010, http://bgpmon.net/blog/?p=323

BIANCA, CESARE MASSIMO ET AL., EU KAUFRECHTS-RICHTLINIE [EU SALES LAW DIRECTIVE] (Stefan Grundmann & Cesare Massimo Bianca eds., 2002)

BISCHOF, PIRMIN, PRODUKTHAFTUNG UND VERTRAG IN DER EU [PRODUCT LIABILITY AND CONTRACT IN THE EU] (1994)

Bishop, Derek A., *To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?*, 3 SHIDLER J. L. COM. & TECH. 7 (2006)

BLACK, JOHN ET AL., A STUDY OF THE MD5 ATTACKS: INSIGHTS AND IMPROVEMENTS (2006), *available at* http://www.cs.colorado.edu/~jrblack/papers/md5e-full.pdf

BLACK'S LAW DICTIONARY (9th ed. 2009)

Blakely, Rhys et al., *MI5 alert on China's cyberspace spy threat*, TIMES, Dec. 1, 2007, *available at* http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece

BLOKDIJK, GERARD & MENKEN, IVANKA, CLOUD COMPUTING – THE COMPLETE CORNERSTONE GUIDE TO CLOUD COMPUTING BEST PRACTICES (2d ed. 2009)

BLOOMENTHAL, HAROLD S., SARBANES-OXLEY ACT IN PERSPECTIVE (2009)

Blumenthal, Marjory S. & Clark, David D., *Rethinking the Design of the Internet: the End-to-End Arguments vs. the Brave New World*, 1 ACM Transactions on Internet Tech. 70 (2001)

Böhme, Rainer & Kataria, Gaurav, *On the Limits of Cyber-Insurance*, *in* Trust and Privacy in Digital Business (Simone Fischer-Hübner et al. eds., 2006)

Borkin, Sheldon, The HIPAA Final Security Standards and ISO/IEC 17799 (2003), http://www.sans.org/reading_room/whitepapers/standards/the_hipaa_final_security_standards_and_iso/iec_17799_1193

Born, Christian, Schadensersatz bei Datenschutzverstößen. Ein ökonomisches Instrument des Datenschutzes und seine präventive Wirkung [Indemnification in the Case of Data Protection Violations. An Economic Instrument of Data Protection and its Preventive Effect] (2001)

Bostelman, John T., 1 The Sarbanes-Oxley Deskbook (2009)

Bostelman, John T., 2 The Sarbanes-Oxley Deskbook (2009)

Bowman, Gerald, *Physical Security for Mission-Critical Facilities and Data Centers*, *in* Information Security Management Handbook 1293 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Braden, R., Requirements for Internet Hosts — Communication Layers, RFC 1122 (1989), ftp://ftp.rfc-editor.org/in-notes/rfc1122.txt

Bradgate, Robert & Twigg-Flesner, Christian, Consumer Sales and Associated Guarantees (2003)

Bradner, S., IETF Working Group Guidelines and Procedures, RFC 2418 (1998), ftp://ftp.rfc-editor.org/in-notes/rfc2418.txt

BRAGG, MELANIE D., HIPAA FOR THE GENERAL PRACTITIONER (2009)

Brand, Oliver, *Probleme mit der „IKEA-Klausel“* [*Problems with the “IKEA clause”*], 2003 ZEITSCHRIFT FÜR DAS GESAMTE SCHULDRECHT 96 (F.R.G.)

Braucher, Jean, *Contracting Out of the Uniform Commercial Code: Contracting Out of Article 2 Using a “License” Label: A Strategy that Should Not Work for Software Products*, 40 LOY. L.A. L. REV. 261 (2006)

Breaux, Travis D. & Baumer, David L., *Legally “Reasonable” Security Requirements: A 10-year FTC Retrospective*, COMPUTERS & SECURITY (forthcoming 2011)

Brennan, Lorin, *Symposium on Approaching E-Commerce Through Uniform Legislation: Understanding the Uniform Computer Information Transactions Act and the Uniform Electronic Transactions Act: Why Article 2 Cannot Apply to Software Transactions*, 38 DUQ. L. REV. 459 (2000)

BREYER, STEPHEN, BREAKING THE VICIOUS CIRCLE: TOWARD EFFECTIVE RISK REGULATION (1993)

Brickey, Kathleen F., *The Magnuson-Moss Act – An Analysis of the Efficacy of Federal Warranty Regulation as a Consumer Protection Tool*, 18 SANTA CLARA L. REV. 73 (1978)

Brill, Jack, *Giving HIPAA Enforcement Room to Grow: Why There Should Not (Yet) Be a Private Cause of Action*, 83 NOTRE DAME L. REV. 2105 (2008)

BROTBY, KRAG, INFORMATION SECURITY GOVERNANCE: A PRACTICAL DEVELOPMENT AND IMPLEMENTATION APPROACH (2009)

BROTBY, W. KRAG, INFORMATION SECURITY MANAGEMENT METRICS: A DEFINITIVE GUIDE TO EFFECTIVE SECURITY MONITORING AND MEASUREMENT (2009)

BROWN, STEPHEN E. ET AL., CRIMINOLOGY: EXPLAINING CRIME AND ITS CONTEXT (7th ed. 2010)

Brühann, Ulf & Zerdick, Thomas, *Umsetzung der EG-Datenschutzrichtlinie* [*Transposition of the EC Data Protection Directive*], 1996 COMPUTER UND RECHT 429 (F.R.G.)

Brusewitz, Alan, *Computing Facility Physical Security, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1339 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Bundesregierung of the Federal Republic of Germany, *Gesetzentwurf der Bundesregierung zum Gesetz zur Modernisierung des Bilanzrechts (BilMoG),* BTDucks 16/10067 (F.R.G.)

Bureau of Nat'l Affairs, *TJX, Financial Institution Plaintiffs Settle Claims in Breach of 46 Million Credit Cards*, 14 ELECTRONIC COM. & L. REP. 1296 (2009)

BUSH, R. & MEYER, D., SOME INTERNET ARCHITECTURAL GUIDELINES AND PHILOSOPHY, RFC 3439 (2002), ftp://ftp.rfc-editor.org/in-notes/rfc3439.txt

CAIN, B. ET AL., INTERNET GROUP MANAGEMENT PROTOCOL, VERSION 3, RFC 3376 (2002), ftp://ftp.rfc-editor.org/in-notes/rfc3376.txt

CAIOLA, ANNE P. ET AL., U.S. DATA BREACH NOTIFICATION LAW: STATE BY STATE (John P. Hutchins ed., 2007)

Cal. Assem. Comm. on Judiciary, *Personal Information: Disclosure: Hearing on A.B. 1298 Before the Assem. Comm. on Judiciary* (Cal. 2007), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_cfa_20070409_110459_asm_comm.html

CAL. DEP'T OF CONSUMER AFF., OFF. OF PRIVACY PROT., RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION (2009), *available at* http://www.privacy.ca.gov/res/docs/pdf/COPP_Breach_Reco_Practices_6-09.pdf

Camp, L. Jean & Wolfram, Catherine, *Pricing Security: A Market In Vulnerabilities, in* ECONOMICS OF INFORMATION SECURITY 17 (L. Jean Camp & Stephen Lewis eds., 2004)

Camp, L. Jean, *The State of Economics of Information Security*, 2 I/S: J.L. & POL'Y 189 (2006)

Carlson, Caron, *Is Network Outage Information a Terror Threat?*, EWEEK.COM, Oct. 4, 2004, http://www.eweek.com/c/a/Government-IT/Is-Network-Outage-Information-a-Terror-Threat

CARNEGIE MELLON UNIV., CMMI® FOR DEVELOPMENT, VERSION 1.2 (2006), *available at* http://www.sei.cmu.edu/reports/06tr008.pdf

CARR, JEFFREY, INSIDE CYBER WARFARE (2009)

Carr, Jim, *Federal agencies' FISMA grade up slightly*, SC MAGAZINE, May 20, 2008, http://www.scmagazineus.com/federal-agencies-fisma-grade-up-slightly/article/110375/

CASAZZA, JACK & DELEA, FRANK, UNDERSTANDING ELECTRIC POWER SYSTEMS: AN OVERVIEW OF TECHNOLOGY, THE MARKETPLACE, AND GOVERNMENT REGULATION (2d ed. 2010)

CENTER FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Chai, John Y., *Medical Device Regulation in the United States and the European Union: A Comparative Study*, 55 FOOD & DRUG L.J. 57 (2000)

Chai, John, *Regulation of Medical Devices in the European Union*, 21 J. LEGAL MED. 537 (2000)

Chandler, Jennifer A., *Improving Software Security: A Discussion of Liability for Unreasonably Insecure Software*, *in* SECURING PRIVACY IN THE INTERNET AGE 155 (Anupam Chander et al. eds., 2008)

Chapman, Gretchen B. & Johnson, Eric J., *Incorporating the Irrelevant: Anchors in Judgments of Belief and Value, in* HEURISTICS AND BIASES: THE PSYCHOLOGY OF INTUITIVE JUDGMENT 120 (Thomas Gilovich et al. eds., 2002)

CHESBROUGH, HENRY, OPEN BUSINESS MODELS: HOW TO THRIVE IN THE NEW INNOVATION LANDSCAPE (2006)

CHESWICK, WILLIAM R. ET AL., FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER (2d ed. 2003)

Childers, Seldon J., Note, *Don't Stop the Music: No Strict Products Liability for Embedded Software*, 19 U. FLA. J.L. & PUB. POL'Y 125 (2008)

CHORIANOPOULOS, ANTONIOS & TSIPTSIS, KONSTANTINOS, DATA MINING TECHNIQUES IN CRM: INSIDE CUSTOMER SEGMENTATION (2009)

CHU, VIVIAN S., CONG. RESEARCH SERV., PRODUCTS LIABILITY: A LEGAL OVERVIEW, CRS REPORT FOR CONGRESS, CRS REPORT FOR CONGRESS R40148 (2009), *available at* http://opencrs.com/document/R40148/2009-01-16/download/1013/

CHUVAKIN, ANTON A. & WILLIAMS, BRANDEN R., PCI COMPLIANCE: UNDERSTAND AND IMPLEMENT EFFECTIVE PCI DATA SECURITY STANDARD COMPLIANCE (2d ed. 2010)

Claburn, Thomas, *Energizer Removes Infected Battery Monitoring Software*, INFORMATIONWEEK, Mar. 8, 2010, *available at* http://www.informationweek.com/news/hardware/desktop/showArticle.jhtml?articleID=223200155

CLARKE, JUSTIN, SQL INJECTION ATTACKS AND DEFENSE (2009)

CLARKE, RICHARD A. & KNAKE, ROBERT K., CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010)

Clotfelter, Charles T., *Private security and the public safety*, 5 J. OF URB. ECON. 388 (1978)

Coffee, John C., *Law and the Market: The Impact of Enforcement*, 156 U. PA. L. REV. 229 (2007)

COHELAN, TIMOTHY D., COHELAN ON CALIFORNIA CLASS ACTIONS (2010-11 ed.)

Collins, David R., *Shrinkwrap, Clickwrap, and Other Software License Agreements: Litigating a Digital Pig in a Poke in West Virginia*, 111 W. VA. L. REV. 531 (2009)

COMM. OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMM'N, INTERNAL CONTROL—INTEGRATED FRAMEWORK (1992)

COMPUTER ECON., MALWARE REPORT 2007: THE ECONOMIC IMPACT OF VIRUSES, SPYWARE, ADWARE, BOTNETS AND OTHER MALICIOUS CODE (2007), *available at* http://www.computereconomics.com/article.cfm?id=1224

Condon, Ron, *Exclusive PCI DSS news: EU regional director rallies UK merchants*, SEARCHSECURITY.CO.UK, Jul. 9, 2010, http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1516495,00.html

CONKLIN, WM. ARTHUR, WHY FISMA FALLS SHORT: THE NEED FOR SECURITY METRICS 8 (SECOND ANNUAL WORKSHOP ON INFORMATION SECURITY AND PRIVACY, 2007), http://www.tech.uh.edu/cae-dc/documents/WISP%202007%20FISMA%20metrics%20paper%20final.pdf

Conner, Cynthia M. et al., *American Health Lawyers Association 2008-2009 Year in Review,* 3 J. HEALTH & LIFE SCI. L. 1 (2009)

Connor, Geoffrey M., *The Financial Services Act of 1999—The Gramm-Leach-Bliley Act*, 71 PA B. ASSN. Q. 29 (2000)

Consumers Union, *Protect your identity*, CONSUMER REPORTS MONEY ADVISER, July 2010, *available at* http://www.consumerreports.org/cro/money/consumer-protection/protect-your-identity/overview/index.htm

Covington, Patricia & Musselman, Meghan, *Privacy and Data Security Developments Affecting Consumer Finance in 2008*, 64 BUS. LAW. 533 (2009)

COWART, ROBERT & KNITTEL, BRIAN, MICROSOFT WINDOWS VISTA IN DEPTH (2008)

Cox, Louis Anthony, *What's Wrong with Risk Matrices?*, 28 RISK ANALYSIS 497 (2008)

Crandall, Rebecca, Recent Development, *Do Computer Purchasers Need Lemon Aid?*, 4 N.C. J.L. & TECH. 307 (2003)

CROSS, MICHAEL, SCENE OF THE CYBERCRIME (2d ed. 2008)

Crumpler, Stewart & Rudolph, Harvey, *FDA Software Policy and Regulation of Medical Device Software*, 52 FOOD & DRUG L.J. 511 (1997)

Culley, Maureen & Allen, Vanessa, *New data blunder as details of thousands of council taxpayers are found on £6.99 computer sold on eBay*, DAILY MAIL (U.K.), Aug. 27, 2008, *available at* http://www.dailymail.co.uk/news/article-1049413/New-data-blunder-details-thousands-council-taxpayers-6-99-sold-eBay.html

Cunningham, Lawrence A., *The Appeal and Limits of Internal Controls to Fight Fraud, Terrorism, Other Ills*, 29 J. CORP. L. 267 (2004)

DALLER, MORTON F., PRODUCT LIABILITY DESK REFERENCE (2009)

DAMMANN, ULRICH & SIMITIS, SPIROS, EG-DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE] (1997)

Danchev, Dancho, *Vodafone HTC Magic shipped with Conficker, Mariposa malware*, ZDNET, Mar. 9, 2010, http://www.zdnet.com/blog/security/vodafone-htc-magic-shipped-with-conficker-mariposa-malware/5626

Darrow, Jonathan J. & Lichtenstein, Stephen D., *"Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age*, 10 N.C. J.L. & TECH. 1 (2008)

Davis, Jason W., *HITECH HIPAA Amendments: New Rules on Breach Notification, Business Associate Compliance, and Enforcement*, HEALTH LAW., June 2009, at 23

De Hert, Paul et al., *Fighting Cybercrime in the Two Europes: The Added Value of the EU Framework Decision and the Council of Europe Convention*, 77 INT'L REV. OF PENAL L. 503 (2006)

de Villiers, Meiring, *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, 30 HASTINGS COMM. & ENT. L.J. 419 (2008)

DEERING, S. & HINDEN, R., INTERNET PROTOCOL, VERSION 6 (IPV6) SPECIFICATION, RFC 2460 (1998), ftp://ftp.rfc-editor.org/in-notes/rfc2460.txt

DENT, KYLE D., POSTFIX: THE DEFINITIVE GUIDE (2003)

Der Spiegel, *IT-Firma versteigert Festplatte mit Millionen Kontodaten* [*IT Company Auctions off Hard Disc Containing Millions of Bank Account Records*], SPIEGEL ONLINE (F.R.G.), Aug. 26, 2008, *available at* http://www.spiegel.de/netzwelt/web/0,1518,574470,00.html

DHANJANI, NITESH ET AL., HACKING: THE NEXT GENERATION (2009)

DIERKS, T. & RESCORLA, E., THE TRANSPORT LAYER SECURITY (TLS) PROTOCOL VERSION 1.2, RFC 5246 (2008), ftp://ftp.rfc-editor.org/in-notes/rfc5246.txt

Dignan, Larry, *Toyota recalls: Is there a patch day for your car in the future?*, ZDNET, Feb. 23, 2010, http://blogs.zdnet.com/BTL/?p=31141

DIRECTORATE GEN. FOR INTERNAL MKT. AND SERVS., CONSULTATION ON THE ADOPTION OF INTERNATIONAL STANDARDS ON AUDITING (2009), *available at* http://ec.europa.eu/internal_market/consultations/docs/2009/isa/consultation_ISAs_en.doc

DIRECTORATE GEN. FOR INTERNAL MKT. AND SERVS., SUMMARY OF COMMENTS: CONSULTATION ON THE ADOPTION OF THE INTERNATIONAL STANDARDS ON AUDITING (2010), *available at* http://ec.europa.eu/internal_market/auditing/docs/isa/isa-final_en.pdf

DOCTER, QUENTIN ET AL., COMPTIA A+ COMPLETE STUDY GUIDE (2009)

Dowell, Michael A., *HHS and FTC Release Guidance on HITECH Act Requirements*, J. HEALTH CARE COMPLIANCE, July-Aug. 2009, at 5

DOYLE, CHARLES, CONG. RESEARCH SERV., CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS, CRS REPORT FOR CONGRESS NO. 97-1025 (2008), *available at* http://www.fas.org/sgp/crs/misc/97-1025.pdf

DRESNER, STEWART & NORCUP, AMY, PRIVACY LAWS & BUSINESS, DATA BREACH NOTIFICATION LAWS IN EUROPE (2009), *available at* http://www.privacylaws.com/templates/EventPage.aspx?id=1410

DUNN, MYRIAM & WIGERT, ISABELLE, INTERNATIONAL CIIP HANDBOOK 2004—AN INVENTORY AND ANALYSIS OF PROTECTION POLICIES IN FOURTEEN COUNTRIES (2004), *available at* http://kms1.isn.ethz.ch/serviceengine/Files/ISN/452/ipublicationdocument_singledocument/72b87f2b-61bd-4122-acbf-4c689532036a/en/doc_454_290_en.pdf

Durney, Edward G., *The Warranty of Merchantability and Computer Software Contracts: A Square Peg Won't Fit in a Round Hole*, 59 WASH. L. REV. 511 (1984)

EASTLAKE, D. & PANITZ, A., RESERVED TOP LEVEL DNS NAMES, RFC 2606 (1999), ftp://ftp.rfc-editor.org/in-notes/rfc2606.txt

Eberle, Edward J., *The Right to Information Self-Determination*, 2001 UTAH L. REV. 965

Eclavea, Romualdo P., *State's standing to sue on behalf of its citizens*, 42 A.L.R. FED. 23 (1979)

Eecke, Patrick Van & Ooms, Barbara, *ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs*, 11 J. INTERNET L. 3 (2007)

Egele, Manuel et al., *Mitigating Drive-By Download Attacks: Challenges and Open Problems, in* iNETSEC 2009 – OPEN RESEARCH PROBLEMS IN NETWORK SECURITY 52 (Jan Camenisch & Dogan Kesdogan eds., 2009)

EHMANN, EUGEN & HELFRICH, MARCUS, EG-DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE] (1999)

Ehmann, Horst & Sutschet, Holger, *EU-Datenschutzrichtlinie – Umsetzungsbedarf und Auswirkungen aus der Sicht des Arbeitsrechts* [*EC Data Protection Directive – Needed Transposition and Effects from a Labor Law Perspective*], 1997 RECHT DER DATENVERARBEITUNG 3 (F.R.G.)

Eichenwald, Kurt & Schiesel, Seth, *S.E.C. Files New Charges On WorldCom*, N.Y. TIMES, Nov. 6, 2002, at C1

Elgie, Nicki K., Note, *The Identity Theft Cat-and-Mouse Game: An Examination of the State and Federal Governments' Latest Maneuvers*, 4 I/S: J. L. & Pol'y for Info. Soc'y 621 (2008)

Elkin-Koren, Niva & Salzberger, Eli M., Law, Economics and Cyberspace: The Effects of Cyberspace on the Economic Analysis of Law (2004)

Ellison, Carl & Schneier, Bruce, *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure*, 16 Computer Security J. 1 (2000), *available at* http://www.schneier.com/paper-pki.pdf

Endorf, Carl F., *Measuring ROI on Security, in* Information Security Management Handbook 133 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Engle, Megan M., *Anti-Spyware Enforcement: Recent Developments*, 3 I/S: J. L. & Pol'y for Info. Soc'y 581 (2008)

European Comm. for Standardization, Secure Signature-Creation Devices "EAL 4+," CEN Workshop Agreement CWA 14169:2002 (2002), *available at* http://www.a-sit.at/pdfs/cwa14169.pdf

European Comm. for Standardization, Secure Signature-Creation Devices "EAL 4+," CEN Workshop Agreement CWA 14169:2004 (2004), *available at* ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14169-00-2004-Mar.pdf

European Comm. for Standardization, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures –Part 1: System Security Requirements, CEN Workshop Agreement CWA 14167-1 (2003), *available at* ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-01-2003-Jun.pdf

EUROPEAN COMM. FOR STANDARDIZATION, SECURITY REQUIREMENTS FOR TRUSTWORTHY SYSTEMS MANAGING CERTIFICATES FOR ELECTRONIC SIGNATURES – PART 2: CRYPTOGRAPHIC MODULE FOR CSP SIGNING OPERATIONS – PROTECTION PROFILE (MCSO-PP), CEN WORKSHOP AGREEMENT CWA 14167-2 (2002)*, available at* http://www.interlex.it/testi/pdf/cwa14167-2.pdf

European Comm'n, *A comprehensive approach on personal data protection in the European Union*, COM (2010) 609 final (Nov. 4, 2010)

European Comm'n, *Amended Commission proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, COM (1992) 442 final (Oct. 15, 1992)

European Comm'n, *Commission communication in the framework of the implementation of the Council Directive 93/42/EEC of 14 June 1993 concerning medical devices*, 2010 O.J. (C 183) 15

European Comm'n, *Commission Communication on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience",* COM (2009) 149 final (Mar. 30, 2009)

European Comm'n, *Commission Communication on Internet governance: the next steps*, COM (2009) 277 final (June 18, 2009)

European Comm'n, *Commission Communication on Network and Information Security: Proposal for A European Policy Approach*, COM (2001) 298 final (June 6, 2001)

European Comm'n, *Commission Communication on new directions on the liability of suppliers of services*, COM (1994) 260 final (June 23, 1994)

European Comm'n, *Commission Communication on Preventing and Combating Corporate and Financial Malpractice*, COM (2004) 611 final (Sept. 27, 2004)

European Comm'n, *Commission Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM (2007) 228 final (May 2, 2007)

European Comm'n, *Commission Communication on Standardization in the European Economy (Follow-up to the Commission Green Paper of October 1990)*, COM (91) 521 final (Dec. 16, 1991)

European Comm'n, *Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security*, COM (90) 314 final (Sept. 13, 1990)

European Comm'n, *Commission Communication, A strategy for a Secure Information Society – "Dialogue, partnership and empowerment,"* COM (2006) 251 final (May 31, 2006)

European Comm'n, *Commission Communication, i2010 – A European Information Society for growth and employment*, COM (2005) 229 final (June 1, 2005)

European Comm'n, *Commission Green Paper on Consumer Collective Redress*, COM (2008) 794 final (Nov. 27, 2008)

European Comm'n, *Commission Green Paper on the Review of the Consumer Acquis*, COM (2006) 744 final (Feb. 8, 2007)

European Comm'n, *Commission Proposal for a Council Directive on the liability of suppliers of services*, COM (1990) 482 final (Dec. 20, 1990)

European Comm'n, *Commission Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of* *personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation*, COM (2007) 698 final (Nov. 13, 2007)

European Comm'n, *Commission Proposal for a Directive of the European Parliament and of the Council amending Council Directives 78/660/EEC and 83/349/EEC concerning the annual accounts of certain types of companies and consolidated accounts*, COM (2004) 725 final (Oct. 27, 2004)

European Comm'n, *Commission Proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services*, COM (2007) 697 final (Nov. 13, 2007)

European Comm'n, *Commission Proposal for a Directive of the European Parliament and of the Council on measures and procedures to ensure the enforcement of intellectual property rights*, COM (2003) 46 final (Jan. 30, 2003)

European Comm'n, *Commission Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, COM (2010) 517 final (Sept. 30, 2010)

European Comm'n, *Commission Proposal for a European Parliament and Council Directive on the sale of consumer goods and associated guarantees*, COM (1995) 520 final (June 18, 1996)

European Comm'n, *Commission Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures*, COM (2006) 120 final (Mar. 15, 2006)

European Comm’n, *Commission Staff Working Document, Impact Assessment,* SEC (2007) 1472 (Nov. 13, 2007)

European Comm’n, *Commission Staff Working Document, Impact Assessment, Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems, and repealing Council Framework Decision 2005/222/JHA*, SEC (2010) 1122 final (Sept. 9, 2010)

European Comm’n, *Commission Staff Working Document—The application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation to the identification of clients in non-face to face transactions and possible implications for electronic commerce*, SEC (2006) 1792 (Dec. 19, 2006)

European Comm’n, *Commission White Paper on Damages actions for breach of the EC antitrust rules,* COM (2008) 165 final (Apr. 2, 2008)

European Comm’n, *Communication from the Commission to the Council and the European Parliament on the implementation of Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees including analysis of the case for introducing direct producers’ liability*, COM (2007) 210 final (Apr. 24, 2007)

European Comm’n, Comparative analysis of the Member States’ and candidate countries’ legislation concerning access to documents (2003), *available at* http://ec.europa.eu/transparency/access_documents/docs/compa_en.pdf

European Comm’n, Consultation Paper for Discussion on the Follow-Up to the Green Paper on Consumer Collective Redress (2009), *available at* http://ec.europa.eu/consumers/redress_cons/docs/consultation_paper2009.pdf

European Comm’n, Europeans and their Languages (2006), *available at* http://ec.europa.eu/public_opinion/archives/ebs/ebs_243_en.pdf

European Comm’n, Feedback Statement summarising the results of the written replies to the Consultation Paper (2009), *available at* http://ec.europa.eu/consumers/redress_cons/docs/overview_results_coll_redress_en.pdf

European Comm’n, *First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, COM (2003) 702 final (Nov. 21, 2003)

European Comm’n, *First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, COM (2003) 702 final (Nov. 21, 2003)

European Comm’n, Guide to the implementation of directives based on the New Approach and the Global Approach (2000), *available at* http://ec.europa.eu/enterprise/policies/single-market-goods/files/blue-guide/guidepublic_en.pdf

European Comm’n, *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*, COM (2008) 448 final (July 14, 2008)

European Comm’n, *Third Commission report on the application of Council Directive 85/374/EEC*, COM (2006) 496 final (Sept. 14, 2006)

EUROPEAN NETWORK & INFO. SEC. AGENCY, DATA BREACH NOTIFICATIONS IN THE EU (2011), *available at* http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport

EUROPEAN NETWORK & INFO. SEC. AGENCY, GUIDELINES FOR ENHANCING THE RESILIENCE OF COMMUNICATION NETWORKS: PROVIDERS' MEASURES (2009), *available at* http://www.enisa.europa.eu/act/res/providers-measures/files/resilience-good-practices/at_download/fullReport

EUROPEAN NETWORK & INFO. SEC. AGENCY, NETWORK PROVIDER MEASURES: RESILIENCE OF COMMUNICATION NETWORKS (2008), *available at* http://www.enisa.europa.eu/act/res/providers-measures/files/network-provider-measures/at_download/fullReport

EUROPEAN NETWORK & INFO. SEC. AGENCY, PROVIDER SECURITY MEASURES PART 1: SECURITY AND ANTI-SPAM MEASURES OF ELECTRONIC COMMUNICATION SERVICE PROVIDERS – SURVEY (2006), *available at* http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures/studies/provider-security-measures-1/at_download/fullReport

EUROPEAN NETWORK & INFO. SEC. AGENCY, SOCIAL ENGINEERING: EXPLOITING THE WEAKEST LINKS (2008), *available at* http://www.enisa.europa.eu/act/ar/deliverables/2008/social-engineering/at_download/fullReport

European Parliament, *Position of the European Parliament adopted at second reading on 6 May 2009*, P6_TA(2009)0360 (May 6, 2009)

EUROPOL, HIGH TECH CRIMES WITHIN THE EU: OLD CRIMES NEW TOOLS, NEW CRIMES NEW TOOLS: THREAT ASSESSMENT 2007 (2007), *available at* http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf

Europol, Threat Assessment (Abridged): Internet Facilitated Organised Crime (2011), *available at* http://www.europol.europa.eu/publications/Serious_Crime_Overviews/Internet%20Facilitated%20Organised%20Crime%20iOCTA.pdf

Eurostat, European Comm'n, Press Release, Nearly one third of internet users in the EU27 caught a computer virus (Feb. 7, 2011), *available at* http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-07022011-AP/EN/4-07022011-AP-EN.PDF

Eustacchio, Andreas, Produkthaftung: Eine systematische Darstellung für die Praxis [Product Liability: A Practical Systematic Outline] (2002)

Falliere, Nicolas et al., Symantec Corp., W32.Stuxnet Dossier (2010), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Farmer, Dan & Venema, Wietse, Forensic Discovery (2004)

Farouk, Mark, Bill Analysis of Assembly Bill 372, 2007-08 Reg. Sess. (Cal. 2008)

FCC, Connecting America: The National Broadband Plan (2010), *available at* http://www.broadband.gov/download-plan/

FCC, FCC Preparedness for Major Public Emergencies (2009), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-293332A1.pdf

Fed. Energy Regulatory Comm'n, Reliability Functional Model: Function Definitions and Functional Entities, Version 5 (2009), *available at* http://www.nerc.com/files/Functional_Model_V5_Final_2009Dec1.pdf

Fed. Fin. Insts. Examination Council, Authentication in an Internet Banking Environment (2005), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf

FED. FIN. INSTS. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK—INFORMATION SECURITY (2006), *available at* http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

FEDERAL TRADE COMM'N, ADVERTISING AND MARKETING ON THE INTERNET: RULES OF THE ROAD (2000), available at http://business.ftc.gov/sites/default/files/pdf/bus28-advertising-and-marketing-internet-rules-road.pdf

Federal Trade Comm'n, FTC Consumer Alert: What To Do If Your Personal Information Has Been Compromised (Mar. 2005), http://ftc.gov/bcp/edu/pubs/consumer/alerts/alt150.shtm

FEDERAL TRADE COMM'N, FTC REPORT TO CONGRESS UNDER SECTIONS 318 AND 319 OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003 (2004), *available at* http://www.ftc.gov/reports/facta/041209factarpt.pdf

Fedtke, Jörg & Magnus, Ulrich, *Germany, in* UNIFICATION OF TORT LAW: STRICT LIABILITY 147 (Bernhard A. Koch & Helmut Koziol, eds., 2002)

Feiler, Lukas, *Data Breach Notification nach österreichischem Recht* [*Data Breach Notification under Austrian Law*], 5 MEDIEN UND RECHT 281 (2009)

Feiler, Lukas, *Neue Bedrohungen aus dem Internet – Botnets: Spamming, Phishing und DDoS Attacks im großen Stil* [*New Internet Threats—Botnets: Spamming, Phishing, and DDoS Attacks on a Large Scale*], ANWALT AKTUELL, Mar. 2007, at 30

Feiler, Lukas, *New Approaches to Network and Information Security Regulation: The EU Telecoms Package*, 2 COMPUTER L. REV. INT'L 43 (2010) (F.R.G.)

Feiler, Lukas, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, 1 EUR. J. OF L. & TECH. 3 (2010), http://ejlt.org//article/view/29/75

FEILER, LUKAS, ZUR STRAFRECHTLICHEN BEURTEILUNG VON IT-SICHERHEITSLÜCKEN [ON THE EVALUATION OF IT SECURITY VULNERABILITIES IN CRIMINAL LAW] (2006), http://lukasfeiler.com/Zur_strafrechtlichen_Beurteilung_von_IT-Sicherheitsluecken.pdf

FERGUSON, NIELS ET AL., CRYPTOGRAPHY ENGINEERING: DESIGN PRINCIPLES AND PRACTICAL APPLICATIONS (2010)

Ferola, Peter, *Internal Controls in the Aftermath of Sarbanes-Oxley: One Size Doesn't Fit All*, 48 S. TEX. L. REV. 87 (2006)

FIELDING, R. ET AL., HYPERTEXT TRANSFER PROTOCOL — HTTP/1.1, RFC 2616 (1999), ftp://ftp.rfc-editor.org/in-notes/rfc2616.txt

FIN. ACCOUNTING STANDARDS BD., *ACCOUNTING FOR CONTINGENCIES*, STATEMENT OF FINANCIAL ACCOUNTING STANDARDS NO. 5 (1975)

FINKLEA, KRISTIN M., CONG. RESEARCH SERV., IDENTITY THEFT: TRENDS AND ISSUES, CRS REPORT FOR CONGRESS R40599 (2010), *available at* http://opencrs.com/document/R40599/2010-01-05/download/1013/

Fitchett, Joseph, *French Report Accuses U.S. of Industrial Sabotage Campaign*, N.Y. TIMES, July 19, 1995, *available at* http://www.nytimes.com/1995/07/19/news/19iht-rivals.html?pagewanted=1

FITZ, HANNS ET AL, PRODUKTHAFTUNG [PRODUCT LIABILITY] (2004)

Fitzgerald, Todd et al., *Information Security and Risk Management, in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 1 (Harold F. Tipton ed., 2007)

Fitzgerald, Todd, *Information Security Governance, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 15 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Florini, Ann, *Introduction: The Battle Over Transparency, in* The Right to Know: Transparency for an Open World 1 (Ann Florini ed., 2007)

Food & Drug Admin., Evaluation of Software Related Recalls for Fiscal Years 1983-91 (1992)

Food & Drug Admin., General Principles of Software Validation; Final Guidance for Industry and FDA Staff (2002), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf

Food & Drug Admin., Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (2005), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089593.pdf

Foster, James C. et al., Buffer Overflow Attacks: Detect, Exploit, Prevent (2005)

Frackman, Andrew et al., Internet and Online Privacy: Legal and Business Guide (2002)

Frank, Sharon, *An Assessment of the Regulations on Medical Devices in the European Union*, 56 Food & Drug L.J. 99 (2001)

Freeman, Jody, *Private Parties, Public Functions and the New Administrative Law*, 52 Admin. L. Rev. 813 (2000)

Freeman, Jody, *The Private Role in Public Governance*, 75 N.Y.U. L. Rev. 543 (2000)

Freiwald, Susan, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9 (2004)

Fried, Ina, *Be sure to read Chrome's fine print*, CNET.COM, Sept. 2, 2008, http://news.cnet.com/8301-13860_3-10030522-56.html?tag=mncol;txt

Fried, Stephen D., *Phishing: A New Twist to an Old Game, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 2853 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Friedman, Stephen E., *Text and Circumstance: Warranty Disclaimers in a World of Rolling Contracts,* 46 ARIZ. L. REV. 677 (2004)

Frischmann, Brett M. & van Schewick, Barbara, *Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo,* 47 JURIMETRICS 383 (2007)

Fromholz, Julia M., *Data Privacy: The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461 (2000)

FULLER, V. & LI, T., CLASSLESS INTER-DOMAIN ROUTING (CIDR): THE INTERNET ADDRESS ASSIGNMENT AND AGGREGATION PLAN, RFC 4632 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4632.txt

FUNG, ARCHON ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY (2007)

Gage, Deborah, *Popular photo frames carry risk of infection*, SAN FRANCISCO CHRONICLE, Jan. 2, 2009, at C1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/01/02/BUV9150IH8.DTL

Gansler, Jacques S. & Lucyshyn, William, *Improving the Security of Financial Management Systems: What are We to Do?*, 24 J. ACCT. & PUB. POL'Y 1 (2005)

GARFINKEL, SIMSON ET AL., PRACTICAL UNIX AND INTERNET SECURITY (3d ed. 2003)

Garfinkel, Simson L., *Risks of Social Security Numbers*, COMMUNICATIONS OF THE ACM, Oct. 1995, at 146

GARFINKEL, SIMSON, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (2000)

GELLENS, R. & KLENSIN, J., MESSAGE SUBMISSION FOR MAIL, RFC 4409 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4409.txt

Gellis, Catherine R., *The State of the Law Regarding Website Owner Liability for User Generated Content*, 66 BUS. LAW. 243 (2010)

Gellman, Barton, *Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say*, WASH. POST, June 27, 2002, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711_pf.html

GENACHOWSKI, JULIUS, CHAIRMAN OF THE FCC, THE THIRD WAY: A NARROWLY TAILORED BROADBAND FRAMEWORK (2010), *available at* http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0506/DOC-297944A1.pdf

GERMAN BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, RISK ANALYSIS BASED ON IT-GRUNDSCHUTZ, BSI-STANDARD 100-3, VERSION 2.5 (2008), *available at* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile

Geva, Benjamin, *Payment Transactions Under the EU Payment Services Directive: A U.S. Comparative Perspective*, 27 PENN ST. INT'L L. REV. 713 (2009)

Ghosh, Shubha & Mangalmurti, Vikram, *Curing Cybersecurity Breaches Through Strict Products Liability*, *in* SECURING PRIVACY IN THE INTERNET AGE 187 (Anupam Chander et al. eds., 2008)

Giardini, Francesca et al, *Overconfidence in Predictions as an Effect of Desirability Bias, in* ADVANCES IN DECISION MAKING UNDER RISK AND UNCERTAINTY 163 (Mohammed Abdellaoui & John D. Hey eds., 2008)

Gilbert, Françoise, *HIPAA Privacy and Security*, *in* A GUIDE TO HIPAA SECURITY AND THE LAW 9 (Stephen S. Wu ed., 2007)

Gillis, Justin & Fountain, Henry, *New Estimates Double Rate of Oil Flowing Into Gulf*, N.Y. TIMES, June 11, 2010, at A1, *available at* http://www.nytimes.com/2010/06/11/us/11spill.html

Gillis, Justin, *Size of Oil Spill Underestimated, Scientists Say,* N.Y. TIMES, May. 14, 2010, at A1, *available at* http://www.nytimes.com/2010/05/14/us/14oil.html

GLASSNER, BARRY, THE CULTURE OF FEAR: WHY AMERICANS ARE AFRAID OF THE WRONG THINGS (1999)

GODBOLE, NINA S., SOFTWARE QUALITY ASSURANCE: PRINCIPLES AND PRACTICE (2004)

Goins, Bonnie A., *Sarbanes–Oxley Compliance: A Technology Practitioner's Guide, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 2693 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

GOLDSMITH, JACK & WU, TIM, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006)

Gomulkiewicz, Robert W., *The Uniform Commercial Code Proposed Article 2B Symposium: The Implied Warranty of Merchantability in Software Contracts: A Warranty no One Dares to Give and How to Change That*, 16 J. Marshall J. Computer & Info. L. 393 (1997)

Goodell, Geoffrey et al., *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing*, *in* 2003 Network and Distributed Systems Security 75, *available at* http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/5.pdf

Goodin, Dan, *Hackers poison well of open-source FTP app: ProFTPD backdoored for 3 days*, The Register, Dec. 2, 2010, http://www.theregister.co.uk/2010/12/02/proftpd_backdoored/

Gordon, Lawrence A., *The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities*, 25 J. of Acct. and Pub. Pol'y 503 (2006)

Gov't Accountability Office, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737 (2007), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-07-737

Gov't Accountability Office, Information Assurance—National Partnership Offers Benefits, but Faces Considerable Challenges, GAO-06-392 (2006), *avaiable at* http://www.gao.gov/new.items/d06392.pdf

Gov't Accountability Office, Privacy: Lessons Learned about Data Breach Notification, GAO-07-657 (2007), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-07-657

Grabow, Geoffrey C., *Preserving Public Key Hierarchy, in* Information Security Management Handbook 1175 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

GRAFF, MARK G. & VAN WYK, KENNETH R., SECURE CODING: PRINCIPLES AND PRACTICES (2003)

GRAHAM, LAWRENCE D., LEGAL BATTLES THAT SHAPED THE COMPUTER INDUSTRY (1999)

GREEN, IAN, DNS SPOOFING BY THE MAN IN THE MIDDLE (2005), *available at* http://www.sans.org/reading_room/whitepapers/dns/dns-spoofing-man-middle_1567

Gross, Grant, *Google's OS Security Claims Called 'idiotic'*, PCWORLD, July 8, 2009, http://www.pcworld.com/businesscenter/article/168087/googles_os_security_claims_called_idiotic.html

GÜNTHER, ANDREAS, PRODUKTHAFTUNG FÜR INFORMATIONSGÜTER [PRODUCT LIABILITY FOR INFORMATION GOODS] (2001)

Guerra, Giorgia, *A Model for Regulation of Medical Nanobiotechnology: The European Status Quo*, 3 NANOTECHNOLOGY L. & BUS. 84 (2006)

Guttman-McCabe, Christopher et al, *Homeland Security and Wireless Telecommunications: The Continuing Evolution of Regulation*, 57 FED. COMM. L.J. 413 (2005)

H. Comm. on Energy and Commerce, *Hewlett-Packard's Pretexting Scandal: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. (2006)

H. Comm. on Energy and Commerce, *The Electric Supply and Transmission Act of 2001: Hearing on H.R. 3406 Before the H. Comm. on Energy and Commerce*, 107th Cong. (2001)

H. Comm. on Government Reform, *Protecting our Nation's Cyber Space: Educational Awareness for the Cyber Citizen: Hearing Before the Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census of the H. Comm. on Government Reform*, 108th Cong. (2004)

H. Comm. on Homeland Security, *Do the Payment Card Industry Data Standards Reduce Cybercrime?: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity and Science and Technology of the H. Comm. on Homeland Security*, 111th Cong. (2009)

HABERSACK, MATHIAS ET AL., 5 MÜNCHNER KOMMENTAR ZUM BÜRGERLICHEN GESETZBUCH [5 MUNICH COMMENTARY OF THE CIVIL CODE] ProdHaftG § 4 recital 37 (Franz Jürgen Säcker & Roland Rixecker eds., 5th ed. 2009)

Hahn, Robert W. & Layne-Farrar, Anne, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283 (2006)

HAMILTON, JAMES & RASMUSSEN, PETER, GUIDE TO INTERNAL CONTROLS UNDER SECTION 404 OF THE SARBANES-OXLEY ACT (2d ed. 2007)

Hansford, Paul, *Physical(Environmental) Security, in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 281 (Harold F. Tipton ed., 2007)

Hanson, Joel B., *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, 4 SHIDLER J. L. COM. & TECH. 11 (2008)

Harden, Blaine & Ahrens, Frank, *Toyota recalls more than 400,000 Priuses, other hybrid cars*, WASHINGTON POST, Feb. 10, 2010, at A12

Harman, Hattie, *Drop-Down Lists and the Communications Decency Act: A Creation Conundrum*, 43 IND. L. REV. 143 (2009)

HARPWOOD, VIVIENNE, MODERN TORT LAW (6th ed. 2005)

HARRIS, SHON, CISSP ALL-IN-ONE EXAM GUIDE (4th ed. 2008)

HARRIS, SHON, CISSP ALL-IN-ONE EXAM GUIDE (5th ed. 2010)

Harvey, Dean William & White, Amy, *Symposium: Exploring Emerging Issues: New Intellectual Property, Information Technology, And Security In Borderless Commerce: The Impact Of Computer Security Regulation On American Companies*, 8 Tex. Wesleyan L. Rev. 505 (2002)

Hassemer, Michael, Heteronomie und Relativität in Schuldverhältnissen [Heteronomy and Relativity in Obligations] (2007)

Hawkinson, J. & Bates, T., Guidelines for creation, selection, and registration of an Autonomous System (AS), RFC 1930 (1996), ftp://ftp.rfc-editor.org/in-notes/rfc1930.txt

Heafey, Richard J. & Kennedy, Don M., Product Liability: Winning Strategies and Techniques (2006)

Healthcare Info. and Mgmt. Sys. Soc'y & Phoenix Health Sys., U.S. Healthcare Industry HIPAA Compliance Survey Results: Summer 2005 (2005), *available at* http://www.himss.org/content/files/Summer_Survey_2005_Final.pdf

Henning-Bodewig, Frauke, Unfair Competition Law: European Union and Member States (2006)

Henry, Kevin, *Risk Management and Analysis, in* Information Security Management Handbook 321 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Herrmann, Debra S., Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI (2007)

Herrmann, Debra S., *The Common Criteria for IT Security Evaluation*, *in* Information Security Management Handbook 1487 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

HILL-ARNING, SUSANNE & HOFFMAN, WILLIAM C., PRODUKTHAFTUNG IN EUROPA [PRODUCT LIABILITY IN EUROPE] (1995)

Hiller, Janine S. et. al., *Due Diligence on the Run: Business Lessons Derived from FTC Actions to Enforce Core Security Principles*, 45 IDAHO L. REV. 283 (2009)

Hillman, Robert A., *U.C.C. Article 2 Express Warranties and Disclaimers In the Twenty-First Century*, 11 DUQ. BUS. L.J. 167 (2009)

HIMES, JAY L., OFFICE OF THE NEW YORK ATTORNEY GENERAL, STATE PARENS PATRIAE AUTHORITY: THE EVOLUTION OF THE STATE ATTORNEY GENERAL'S AUTHORITY (2004), *available at* http://www.abanet.org/antitrust/at-committees/at-state/pdf/publications/other-pubs/parens.pdf

Hirsch, Reece, *New California Information Security Law Will Have National Impact*, 9 ELECTRONIC COM. & L. REP. 905 (2004)

HÖFFE, SIBYLLE, DIE VERBRAUCHSGÜTERKAUFRICHTLINIE 1999/44/EG UND IHRE AUSWIRKUNGEN AUF DEN SCHADENSERSATZ BEIM KAUF [THE CONSUMER SALES DIRECTIVE 1999/44/EC AND ITS EFFECTS ON SALES CONTRACT LIABILITY] (2002)

HOFFMAN, PAUL S., THE SOFTWARE LEGAL BOOK (2003)

Hoffman, Sharona & Podgurski, Andy, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV 331 (2007)

Hoffman, Sharona & Podgurski, Andy, *Information Security of Health Data, in* HARBORING DATA: INFORMATION SECURITY LAW AND THE CORPORATION 103 (Andrea M. Matwyshyn ed., 2009)

Hofman, Mark, *AVG Update Bricking windows 7 64 bit*, SANS INTERNET STORM CENTER, Dec. 3, 2010, http://isc.sans.edu/diary.html?storyid=10030

HOFMANN, MARKUS & BEAUMONT, LELAND, CONTENT NETWORKING: ARCHITECTURE, PROTOCOLS, AND PRACTICE (2005)

HOGLUND, GREG & BUTLER, JAMIE, ROOTKITS: SUBVERTING THE WINDOWS KERNEL (2005)

Hoitash, Udi et al., *Corporate Governance and Internal Control over Financial Reporting: A Comparison of Regulatory Regimes*, 84 ACCT. REV. 839 (2009)

Hollmann, Hermann, *Die EG-Produkthaftungsrichtlinie* [*The EC Product Liability Directive*], 1985 DER BETRIEB 2439 (F.R.G.)

Homburger, Adolf, *State Class Actions and the Federal Rule*, 71 COLUM. L. REV. 609 (1971)

Honeywill, Sean C., *Data Security and Data Breach Notification for Financial Institutions*, 10 N.C. BANKING INST. 269 (2006)

HOOFNAGLE, CHRIS ET AL., HOW DIFFERENT ARE YOUNG ADULTS FROM OLDER ADULTS WHEN IT COMES TO INFORMATION PRIVACY ATTITUDES AND POLICIES? (2010), http://ssrn.com/abstract=1589864

Hoofnagle, Chris Jay, *Internalizing Identity Theft*, 13 UCLA J. L. TECH. 2 (2009), *available at* http://lawtechjournal.com/articles/2009/02_100406_Hoofnagle.pdf

HOOFNAGLE, CHRIS JAY, PRIVACY SELF REGULATION: A DECADE OF DISAPPOINTMENT (2005), *available at* http://epic.org/reports/decadedisappoint.pdf

Hoofnagle, Chris Jay, *Putting Identity Theft on Ice: Freezing Credit Reports To Prevent Lending to Impostors, in* SECURING PRIVACY IN THE INTERNET AGE 207 (Anupam Chander et al. eds., 2008)

Hooper, John & Milner, Mark, *Parmalat debacle predicted to cost Italian economy €11bn*, THE GUARDIAN (U.K.), Jan. 15, 2004, *available at* http://www.guardian.co.uk/business/2004/jan/15/corporatefraud.italy1

Hoover, Nicholas, *White House Updates Cybersecurity Orders*, INFORMATIONWEEK, Apr. 21, 2010, http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=224500173&subSection=News

Horney, Julie & Marshall, Ineke, *Risk Perceptions Among Serious Offenders: The Role of Crime and Punishment*, 30 CRIMINOLOGY 575 (1992)

Horovitz, Bonna Lynn, *Computer Software as a Good under the Uniform Commercial Code: Taking a Byte out of the Intangibility Myth*, 65 B.U.L. REV. 129 (1985)

Horton, Linda R., *Medical Device Regulation in the European Union*, 50 FOOD & DRUG L.J. 461 (1995)

HORWATH, CHRISTIAN, SOFTWARE UND PRODUKTHAFTUNG [SOFTWARE AND PRODUCT LIABILITY] (2002)

Houwen, Joost, *Methods of Attacking and Defending Cryptosystems, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1255 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

HOWARD, MICHAEL & LIPNER, STEVE, THE SECURITY DEVELOPMENT LIFECYCLE: SDL: A PROCESS FOR DEVELOPING DEMONSTRABLY MORE SECURE SOFTWARE (2006)

HOWARD, PATRICK D., BUILDING AND IMPLEMENTING A SECURITY CERTIFICATION AND ACCREDITATION PROGRAM: OFFICIAL (ISC)^2 GUIDE TO THE CAP CBK (2006)

Hubbard, Douglas D. & Samuelson, Douglas A., *Modeling Without Measurements: How the decision analysis culture's lack of empiricism reduces its effectiveness*, OR/MS Today, Oct. 2009, at 26

Hubbard, Douglas W., How to Measure Anything: Finding the Value of Intangibles in Business (2d ed. 2010)

Hubbard, Douglas W., The Failure of Risk Management: Why It's Broken and How to Fix It (2009)

Idaho Nat'l Laboratory, NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses (2010), *available at* http://www.fas.org/sgp/eprint/nstb.pdf

Identity Theft Res. Ctr., 1st Annual Identity Theft Resource Center "Consumer Internet Transaction Concerns" Survey (2010), http://www.idtheftcenter.org/artman2/uploads/1/Consumer_Concerns_Survey_20100813.pdf

Ikbal, Javek, *An Introduction to Cryptography, in* Information Security Management Handbook 1121 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Inst. of Electrical and Electronics Engineers, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, IEEE 802.3-2008 (2008), *available at* http://standards.ieee.org/getieee802/802.3.html

Inst. of Electrical and Electronics Engineers, IEEE Standard for Information technology—Telecommunications and information exchange between systems—

Local and metropolitan area networks—Specific requirements—Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, IEEE 802.3-2008 (2008), *available at* http://standards.ieee.org/getieee802/802.3.html

Int'l Auditing & Assurance Standards Bd., Communicating Deficiencies in Internal Control to Those Charged with Governance and Management, International Standard on Auditing 265 (2009), *available at* http://web.ifac.org/download/a015-2010-iaasb-handbook-isa-265.pdf

Int'l Electrotechnical Comm'n, International Electrotechnical Vocabulary - Chapter 191: Dependability and Quality of Service, IEC 60050-191 (1990)

Int'l Electrotechnical Comm'n, Medical device software – Software life cycle processes, IEC 62304:2006 (2006)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary, ISO/IEC 27000:2009 (2009)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model, ISO/IEC 7498-1:1994 (1994)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information processing systems — Fibre distributed Data Interface (FDDI) — Part 3: Physical Layer Medium Dependent (PMD), ISO/IEC 9314-3:1990 (1990)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information technology – Security techniques – Code of practice for information security management, ISO/IEC 27002:2005 (2005)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information technology – Security techniques – Information security management – Measurement, ISO/IEC 27004:2009 (2009)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2008 (2008)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, ISO/IEC 13335-1:2004 (2004)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, ISO/IEC 15408-1:2009 (2009)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001:2005 (2005)

Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components, ISO/IEC 15408-2:2008 (2008)

INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – EVALUATION CRITERIA FOR IT SECURITY – PART 3: SECURITY ASSURANCE COMPONENTS, ISO/IEC 15408-3:2008 (2008)

INT'L ORG. FOR STANDARDIZATION, INFORMATION PROCESSING SYSTEMS — FIBRE DISTRIBUTED DATA INTERFACE (FDDI) — PART 1: TOKEN RING PHYSICAL LAYER PROTOCOL (PHY), ISO 9314-1:1989 (1989)

INT'L ORG. FOR STANDARDIZATION, INFORMATION PROCESSING SYSTEMS — FIBRE DISTRIBUTED DATA INTERFACE (FDDI) — PART 2: TOKEN RING MEDIA ACCESS CONTROL (MAC), ISO 9314-2:1989 (1989)

INT'L ORG. FOR STANDARDIZATION, INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT GUIDELINES FOR TELECOMMUNICATIONS ORGANIZATIONS BASED ON ISO/IEC 27002, ISO/IEC 27011:2008 (2008)

INT'L ORG. FOR STANDARDIZATION, QUALITY MANAGEMENT SYSTEMS – FUNDAMENTALS AND VOCABULARY, ISO 9000:2005 (2005)

INT'L ORG. FOR STANDARDIZATION, QUALITY MANAGEMENT SYSTEMS – REQUIREMENTS, ISO 9001:2008 (2008)

INT'L ORG. FOR STANDARDIZATION, MEDICAL DEVICES – QUALITY MANAGEMENT SYSTEMS – REQUIREMENTS FOR REGULATORY PURPOSES, ISO 13485:2003/Cor 1:2009 (2009)

INT'L TELECOMM. UNION, INTRODUCTION TO CCITT SIGNALLING SYSTEM NO. 7, ITU-T RECOMMENDATION Q.700 (1993), *available at* http://www.itu.int/rec/T-REC-Q.700-199303-I/en

INT'L TELECOMM. UNION, PACKET-BASED MULTIMEDIA COMMUNICATIONS SYSTEMS, ITU-T RECOMMENDATION H.323 (2009), *available at* http://www.itu.int/rec/T-REC-H.323-200912-P/en

INT'L TELECOMM. UNION, QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING – TERMS AND DEFINITIONS RELATED TO THE QUALITY OF TELECOMMUNICATION SERVICES, ITU-T RECOMMENDATION E.800 (2008), *available at* http://www.itu.int/rec/T-REC-E.800-200809-I/en

Ionescu, Daniel, *Microsoft Red-Faced After Massive Sidekick Data Loss*, PCWORLD, Oct. 12, 2009, *available at* http://www.pcworld.com/article/173470/microsoft_redfaced_after_massive_sidekick_data_loss.html

IT GOVERNANCE INST., CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT) 4.1 (2007), *available at* http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf (registration required)

Jackson, Carl B., *Business Continuity and Disaster Recovery Planning, in* OFFICIAL (ISC)^2 GUIDE TO THE CISSP CBK 337 (Harold F. Tipton ed., 2007)

Jackson, William, *Effective IT security starts with risk analysis, former GAO CTO says*, GOV'T COMPUTER NEWS, June 19, 2009, http://gcn.com/Articles/2009/06/15/Interview-Keith-Rhodes-IT-security.aspx?sc_lang=en&Page=2

Jackson, William, *FISMA's effectiveness questioned*, GOV'T COMPUTER NEWS, Mar. 18, 2007, http://gcn.com/Articles/2007/03/18/FISMAs-effectiveness-questioned.aspx?Page=1

JAQUITH, ANDREW, SECURITY METRICS: REPLACING FEAR, UNCERTAINTY, AND DOUBT (2007)

JENTZSCH, NICOLA, FINANCIAL PRIVACY: AN INTERNATIONAL COMPARISON OF CREDIT REPORTING SYSTEMS (2d ed. 2007)

Joerges, Christian et al., The Law's Problems with the Involvement of Non-Governmental Actors in Europe's Legislative Processes: The Case of Standardisation under the 'New Approach,' EUI Working Paper LAW No. 99/9 (1999), *available at* http://cadmus.eui.eu/bitstream/handle/1814/154/law99_9.pdf?sequence=1

Johnson, Vincent R., *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. Rev. 255 (2005)

Jones, Edward, *Introduction to DSL, in* Fundamentals of DSL Technology 119 (Philip Golden et al. eds., 2006)

Jones, George, *The 10 Most Destructive PC Viruses Of All Time*, InformationWeek, July 5, 2006, http://www.informationweek.com/news/windows/security/showArticle.jhtml?articleID=190300173

Jones, Jeffrey R., Microsoft. Inc., Browser Vulnerability Analysis of Internet Explorer and Firefox (2007), *available at* http://blogs.technet.com/cfs-file.ashx/__key/CommunityServer-Components-PostAttachments/00-02-59-48-22/ie_2D00_firefox_2D00_vuln_2D00_analysis.pdf

Jorden, Simone, Verbrauchergarantien [Consumer Guarantees] (2001)

Julià-Barceló, Rosa & Koelman, Kamiel J., *Intermediary Liability in the E-Commerce Directive: So Far So Good, But It's Not Enough*, 16 Computer L. & Security Rep. 231 (2000)

Juran, Joseph M., *Attaining Superior Results through Quality, in* Juran's Quality Handbook 33 (Joseph M. Juran & Joseph A. De Feo eds., 6th ed. 2010)

Kahn, Benita A. & Enlow, Heather J., *The Federal Trade Commission's Expansion of the Safeguards Rule*, Fed. Law., Sept. 2007, at 39, *available at* 54-SEP Fed. Law. 39 (Westlaw)

Kaplan, Dan, *TJX breach began in Minnesota Marshalls parking lot*, SC MAGAZINE, May 4, 2007, http://www.scmagazineus.com/report-tjx-breach-began-in-minnesota-marshalls-parking-lot/article/34954/

Kaplan, David A., *Suspicions and Spies in Silicon Valley*, NEWSWEEK, Sept. 18, 2006, *available at* http://www.newsweek.com/2006/09/17/suspicions-and-spies-in-silicon-valley.html

KAU, CHRISTIAN, VERTRAUENSSCHUTZMECHANISMEN IM INTERNET, INSBESONDERE IM E-COMMERCE [PROTECTION OF LEGITIMATE EXPECTATION ON THE INTERNET, PARTICULARLY IN E-COMMERCE] (2006)

KAUTZ, ILONA, SCHADENSERSATZ IM EUROPÄISCHEN DATENSCHUTZRECHT [INDEMNIFICATION UNDER EUROPEAN DATA PROTECTION LAW] (2006)

Keizer, Gregg, *Conficker cashes in, installs spam bots and scareware*, COMPUTERWORLD, Apr. 9, 2009, http://www.computerworld.com/s/article/9131380/Conficker_cashes_in_installs_spam_bots_and_scareware?taxonomyName=Security

Keizer, Gregg, *Symantec false positive cripples thousands of Chinese PCs*, COMPUTERWORLD, May 18, 2007, http://www.computerworld.com/s/article/9019958/Symantec_false_positive_cripples_thousands_of_Chinese_PCs

Kenneally, Erin, *Stepping on the Digital Scale: Duty and Liability for Negligent Internet Security*, 26 ;LOGIN 62 (2001)

Kenneally, Erin, *The Byte Stops Here: Duty and Liability for Negligent Internet Security*, 16 COMPUTER SECURITY J. 1 (2000), *available at* http://web.archive.org/web/20040623113244/http://www.allasso.pt/base/docs/11022984657.pdf

KENNEDY, CHARLES H., AN INTRODUCTION TO U.S. TELECOMMUNICATIONS LAW (2d ed. 2001)

Kennedy, John B., *Slouching Towards Security Standards: The Legacy Of California's SB 1386*, 865 PLI/PAT 91 (2006)

Kent, Stephen et al., *Secure Border Gateway Protocol (S-BGP)*, 18 IEEE J. ON SELECTED AREAS IN COMM. 582 (2000)

Kerr, Orin S., *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003)

Kiefer, Kimberly & Sabett, Randy V., *Openness of Internet Creates Potential for Corporate Information Security Liability*, 7 ELECTRONIC COM. & L. REP. 594 (2002)

KIEFER, KIMBERLY ET AL., INFORMATION SECURITY: A LEGAL, BUSINESS, AND TECHNICAL HANDBOOK (2004)

Kincaid, Jason, *Facebook Bug Reveals Private Photos, Wall Posts*, WASHINGTONPOST.COM, Mar. 20, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/03/21/AR2009032104050.html

Kincaid, Jason, *Google Privacy Blunder Shares Your Docs Without Permission*, TECHCRUNCH.COM, Mar. 7, 2009, http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/

KLENSIN, J., SIMPLE MAIL TRANSFER PROTOCOL, RFC 5321 (2008), ftp://ftp.rfc-editor.org/in-notes/rfc5321.txt

Kobayashi, Bruce K., *Private versus Social Incentives in Cybersecurity: Law and Economics, in* THE LAW AND ECONOMICS OF CYBERSECURITY 13 (Mark F. Grady & Francesco Parisi eds., 2006)

Koch, Bernhard A., *Punitive Damages in European Law, in* Punitive Damages: Common Law and Civil Law Perspectives 197 (Helmut Koziol & Vanessa Wilcox eds., 2009)

Köhler, Annette et al., Evaluation of the Possible Adoption of International Standards on Auditing (ISAs) in the EU (2009), *available at* http://ec.europa.eu/internal_market/auditing/docs/ias/study2009/report_en.pdf

Kopp, Ferdinand, *Das EG-Richtlinienvorhaben zum Datenschutz – Geänderter Vorschlag der EG-Kommission für eine „Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“* [*The EC Directive Proposal About Data Protection—Amended Commission Proposal for an “amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data“*], 1993 Recht der Datenverarbeitung 1 (F.R.G.)

Korff, Douwe, EC Study on Implementation of Data Protection Directive—Comparative Summary of National Laws (2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf

Korff, Douwe, Study on Implementation of Data Protection Directive – Comparative Summary of National Laws (2002), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf

Kort, Michael, *Produkteigenschaft medizinischer Software: Einordnung im deutschen und US-amerikanischen Produkthaftungsrecht* [*Medical Software as Products: Classification Under German and U.S. Product Liability Law*] 1990 Computer und Recht 171 (F.R.G.)

Kosmides, Timoleon, Zivilrechtliche Haftung für Datenschutzverstöße [Civil Liability for Data Protection Violations] (2010)

KRANENBORG, HERKE & VOERMANS, WIM, ACCESS TO INFORMATION IN THE EUROPEAN UNION: A COMPARATIVE ANALYSIS OF EC AND MEMBER STATE LEGISLATION (2005)

Krebs, Brian, *Blogfight: IE Vs. Firefox Security*, WASH. POST, Jan. 29, 2009, http://voices.washingtonpost.com/securityfix/2009/01/blogfight_the_truth_about_ie_v.html

Krebs, Brian, *Internet Explorer Unsafe for 284 Days in 2006*, WASH. POST, Jan. 4, 2007, http://blog.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html

Krebs, Brian, *Verizon to Implement Spam Blocking Measures*, WASH. POST, Feb. 27, 2009, http://voices.washingtonpost.com/securityfix/2009/02/verizon_to_implement_spam_bloc.html

Krehnke, Mollie E. & Krehnke, David C., *Sensitive or Critical Data Access Controls, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 739 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

KREINDLER, LEE S. ET AL., 15 NEW YORK LAW OF TORTS (2010)

Kugler, Richard L., *Deterrence of Cyber Attacks, in* CYBERPOWER AND NATIONAL SECURITY 309 (Franklin D. Kramer et al. eds., 2009)

KULLMANN, HANS JOSEF, PRODUKTHAFTUNGSGESETZ [PRODUCT LIABILITY ACT] (3d ed. 2001)

Kumar, Dhananjay et al., *Availability Modelling of the 3GPP R99 Telecommunication Networks, in* SAFETY & RELIABILITY 977 (Bedford & van Gelder eds., 2003), *available at* http://www.nokia.com/library/files/docs/Availability_Modelling_of_3GPP_R99_Telecommunication_Networks.pdf

Kuwahara, Emily, *Torts v. Contracts: Can Microsoft Be Held Liable to Home Consumers For Its Security Flaws?*, 80 S. CAL. L. REV. 997 (2007)

Lachow, Irving, *Cyber Terrorism: Menace or Myth?, in* CYBERPOWER AND NATIONAL SECURITY 437 (Franklin D. Kramer et al. eds., 2009)

LANDOLL, DOUGLAS J., THE SECURITY RISK ASSESSMENT HANDBOOK (2006)

LANDWELL & ASSOCIÉS, STUDY ON MONITORING AND ENFORCEMENT PRACTICES IN CORPORATE GOVERNANCE IN THE MEMBER STATES: DETAILED LEGAL ANALYSIS (2009), *available at* http://ec.europa.eu/internal_market/company/docs/ecgforum/studies/comply-or-explain-090923-appendix1_en.pdf

LANDY, GENE K. & MASTORBATTISTA, AMY J., THE IT / DIGITAL LEGAL COMPANION: A COMPREHENSIVE BUSINESS GUIDE TO SOFTWARE, IT, INTERNET, MEDIA AND IP LAW (2008)

Langevoort, Donald C., *Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's "Duty of Care As Responsibility for Systems"*, 31 J. CORP. L. 949 (2006)

Langevoort, Donald C., *Resetting the Corporate Thermostat: Lessons from the Recent Financial Scandals About Self-Deception, Deceiving Others and the Design of Internal Controls,* 93 GEO. L.J. 285 (2004)

Langevoort, Donald C., *Symposium: Robert Clark's Corporate Law: Twenty Years of Change: Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's "Duty of Care as Responsibility for Systems"*, 31 IOWA J. CORP. L. 949 (2006)

Lannan, Jacquetta, *Saving 17200: An Analysis of Proposition 64*, 46 SANTA CLARA L. REV. 451 (2006)

LARSEN, LESLIE M. ET AL., 13A CALIFORNIA JURISPRUDENCE 3D (2010)

LAW REFORM COMM'N OF CANADA, FEAR OF PUNISHMENT: DETERRENCE (1976)

Lee, Christopher & Goldfarb, Zachary A., *Stolen VA Laptop and Hard Drive Recovered*, WASH. POST, June 30, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/29/AR2006062900352.html

Legislative Development, *Scope of the E-Commerce Directive 2000/31/EC of June 8, 2000*, 7 COLUM. J. EUR. L. 473, 475 (2001)

Lehmann, Michael, *Produkt- und Produzentenhaftung für Software* [*Product and Producer Liability for Software*], 1992 NEUE JURISTISCHE WOCHENSCHRIFT 1721 (F.R.G.)

Lelarge, Marc & Bolot, Jean, *Network Externalities and the Deployment of Security Features and Protocols in the Internet*, 2008 ACM SIGMETRICS 37

Lemos, Robert, *Microsoft warns of hijacked certificates*, CNET.COM, Mar. 22, 2001, http://news.cnet.com/2100-1001-254586.html&tag=tp_pr

LESSIG, LAWRENCE, CODE: VERSION 2.0 (2006)

LESSIG, LAWRENCE, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (2001)

Leviant, H. Scott, *Unintended Consequences: How the Passage of Ballot Proposition 64 May Increase the Number of Successful Wage and Hour Class Actions in California*, 6 U.C. DAVIS BUS. L.J. 183 (2006)

LEVINE, JOHN R., QMAIL (2004)

LEVY, STEVEN, HACKERS: HEROES OF THE COMPUTER REVOLUTION (1984)

Leyden, John, *Rogue McAfee update strikes police, hospitals and Intel*, THE REGISTER, Apr. 22, 2010, http://www.theregister.co.uk/2010/04/22/mcafee_false_positive_analysis/

Lichtenstein, Sarah et al., *Calibration of probabilities: The state of the art to 1980, in* JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES 306 (Daniel Kahneman et al. eds., 1982)

Lichtman, Doug & Posner, Eric P., *Holding Internet Service Providers Accountable, in* THE LAW AND ECONOMICS OF CYBERSECURITY 221 (Mark F. Grady & Francesco Parisi eds., 2006)

LIGHT, PAUL C., THICKENING GOVERNMENT: FEDERAL HIERARCHY AND THE DIFFUSION OF ACCOUNTABILITY (1995)

LIU, CRICKET & ALBITZ, PAUL, DNS AND BIND (5th ed. 2006)

LIU, CRICKET ET AL., DNS ON WINDOWS SERVER 2003 (2003)

LONG, JOHNNY, NO TECH HACKING: A GUIDE TO SOCIAL ENGINEERING, DUMPSTER DIVING, AND SHOULDER SURFING (2008)

LOVELLS, PRODUCT LIABILITY IN THE EUROPEAN UNION: A REPORT FOR THE EUROPEAN COMMISSION (2003), *available at* http://ec.europa.eu/enterprise/policies/single-market-goods/files/goods/docs/liability/studies/lovells-study_en.pdf

Lukmire, David, *Can the Courts Tame the Communications Decency Act?: The Reverberations of Zeran v. America Online*, 66 N.Y.U. ANN. SURV. AM. L. 371 (2010)

Lyon, David, *Surveillance as social sorting: computer codes and mobile bodies, in* SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK AND AUTOMATED DISCRIMINATION 13 (David Lyon ed., 2003)

MacCarthy, Mark, *Payment Card Industry Data Security Standard, in* PROSKAUER ON PRIVACY § 16 (Kristen J. Mathews ed., 2010)

Majoras, Deborah Platt, Chairman, Fed. Trade Comm’n, Remarks at the Progress and Freedom Foundation Securing the Internet Project Internet Security Summit (May 10, 2006), *available at* http://www.ftc.gov/speeches/majoras/060510ProgressFreedomFoundationRev 051006

MALHOTRA, RAVI, IP ROUTING (2002)

MANN, SCOTT & MITCHELL, ELLEN L., LINUX SYSTEM SECURITY: THE ADMINISTRATOR'S GUIDE TO OPEN SOURCE SECURITY TOOLS (2d ed. 2000)

MARCUS, EVAN & STERN, HAL, BLUEPRINTS FOR HIGH AVAILABILITY (2003)

MARCUS, EVAN & STERN, HAL, BLUEPRINTS FOR HIGH AVAILABILITY: DESIGNING RESILIENT DISTRIBUTED SYSTEMS (2000)

Markoff, John, *Worm Infects Millions of Computers Worldwide*, N.Y. TIMES, Jan. 22, 2009, at A12, *available at* http://www.nytimes.com/2009/01/23/technology/internet/23worm.html

Markus, Stephen L., Note, *Unfair Warning: Breach Notification in The FCC’s Enhanced Telephone Records Safeguards,* 18 CORNELL J.L. & PUB. POL’Y 247 (2008)

Marsan, Carolyn Duffy, *Six worst Internet routing attacks*, NETWORK WORLD, Jan. 15, 2009, http://www.networkworld.com/news/2009/011509-bgp-attacks.html

Mathewson, Nancy W., *Prohibited Acts and Enforcement Tools*, 65 FOOD & DRUG L.J. 545 (2010)

Maule, Michael R., Comment, *Applying Strict Product Liability to Computer Software*, 27 TULSA L.J. 735 (1992)

Mayer, Kurt, *Das neue Produkthaftungsrecht* [*The New Product Liability Law*], 1990 VERSICHERUNGSRECHT 691 (F.R.G.)

MCCONNELL, STEVE, CODE COMPLETE: A PRACTICAL HANDBOOK OF SOFTWARE CONSTRUCTION (2d ed. 2004)

McCoy, R. Scott, *Perimeter Security, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1275 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

MCCUMBER, JOHN, ASSESSING AND MANAGING SECURITY RISK IN IT SYSTEMS: A STRUCTURED METHODOLOGY (2005)

McGhie, Lynda L., *Health Insurance Portability and Accountability Act Security Rule*, *in* INFORMATION SECURITY MANAGEMENT HANDBOOK 2703 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

MCGRAW, GARY, SOFTWARE SECURITY: BUILDING SECURITY IN (2006)

McMillan, Robert, *Siemens warns users: Don't change passwords after worm attack*, INFOWORLD, July 10, 2010, http://www.infoworld.com/d/security-central/siemens-warns-users-dont-change-passwords-after-worm-attack-915?page=0,0&source=rss_security_central

McNulty, Patrick J., *The Public Disclosure of Private Facts: There Is Life After Florida Star*, 50 DRAKE L. REV. 93 (2001)

Mead, Nancy R., *Who Is Liable for Insecure Systems?*, 37 COMPUTER 27 (2004)

MELL, PETER ET AL., A COMPLETE GUIDE TO THE COMMON VULNERABILITY SCORING SYSTEM VERSION 2.0 (2007), *available at* http://www.first.org/cvss/cvss-guide.pdf

Mell, Peter et al., *Common Vulnerability Scoring System*, IEEE SECURITY & PRIVACY, Nov. 2006, at 85

Mende, Daniel et al., ERNW, All Your Packets Are Belong to Us □ Attacking Backbone Technologies (2009), *available at* http://www.ernw.de/content/e7/e181/e1309/download1360/ERNW_White_paper_All_your_packets_ger.pdf

Michener, John R. et. al., *"Snake-Oil Security Claims" The Systematic Misrepresentation of Product Security in the E-Commerce Arena*, 9 Mich. Telecomm. & Tech. L. Rev. 211 (2003)

Micklitz, Hans-W., Regulatory Strategies on Services Contracts in EC Law, EUI Working Paper Law No. 2008/06 (2008), *available at* http://ssrn.com/abstract=1093643

Microsoft Corp., Microsoft Security Development Lifecycle (SDL) – Version 5.0 (2010), *available at* http://www.microsoft.com/downloads/details.aspx?FamilyID=7d8e6144-8276-4a62-a4c8-7af77c06b7ac&displaylang=en

Mihm, Stephen, *Dumpster-Diving for Your Identity*, N.Y. Times, Dec. 21, 2003, *available at* http://www.nytimes.com/2003/12/21/magazine/dumpster-diving-for-your-identity.html?partner=rssnyt&emc=rss&pagewanted=1

Milewski, Anthony D. Jr., *Compliance with California Privacy Laws: Federal Law also Provides Guidance to Businesses Nationwide*, 2 Shidler J. L. Com. & Tech. 19 (2006)

Miller, Chuck, *U.S. Veteran Affairs Department settles data breach case*, SC Magazine, Jan. 28, 2009, *available at* http://www.scmagazineus.com/us-veteran-affairs-department-settles-data-breach-case/article/126518/

Miller, James C. III, Chairman, FTC, Letter from, to John D. Dingell, Chairman, Subcommittee on Oversight and Investigations, Committee on Energy and Commerce (Oct. 14, 1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm

Mills, D.L., Exterior Gateway Protocol Formal Specification, RFC 904 (1984), ftp://ftp.rfc-editor.org/in-notes/rfc904.txt

Mills, Elinor, *Twitter's network gets breached again*, CNET.COM, May 1, 2009, http://news.cnet.com/8301-1009_3-10231847-83.html?tag=mncol;txt

MILONE, MARK G., INFORMATION SECURITY LAW: CONTROL OF DIGITAL ASSETS (2009)

MINORITY STAFF OF H.R. COMM. ON GOV'T REFORM, 108TH CONG., SECRECY IN THE BUSH ADMINISTRATION (2004), *available at* http://www.fas.org/sgp/library/waxman.pdf

MITNICK, KEVIN D. & SIMON, WILLIAM L., THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY (2002)

Mitts, James S., *Testing Business Continuity and Disaster Recovery Plans, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1629 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Miyaki, Patrick T., Comment, *Computer Software Defects: Should Computer Software Manufacturers Be Held Strictly Liable for Computer Software Defects?*, 8 SANTA CLARA COMPUTER & HIGH TECH. L.J. 121 (1992)

MOCKAPETRIS, P., DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION, RFC 1035 (1987), ftp://ftp.rfc-editor.org/in-notes/rfc1035.txt

MOELLER, ROBERT R., SARBANES-OXLEY INTERNAL CONTROLS: EFFECTIVE AUDITING WITH AS5, COBIT, AND ITIL (2008)

MORITZ, HANS-WERNER & TYBUSSECK, BARBARA, COMPUTERSOFTWARE [COMPUTER SOFTWARE] (2d ed. 1992)

Morse, Edward A. & Raval, Vasant, *PCIDSS and the Legal Framework for Security: An Update on Recent Developments and Policy Directions,* 1 LYDIAN PAYMENTS J. 31 (2010)

Movius, Lauren B. & Krup, Nathalie, *U.S. and EU Privacy Policy: Comparison of Regulatory Approaches,* 3 Int'l J. of Comm. 169 (2009)

Mozilla Found., *Critical Vulnerability in Microsoft Metrics*, Mozilla Security Blog, Nov. 30, 2007, http://blog.mozilla.com/security/2007/11/30/critical-vulnerability-in-microsoft-metrics/

Mueller, Milton L., Ruling the Root: Internet Governance and the Taming of Cyberspace (2002)

Murdock, Charles W., *Sarbanes-Oxley Five Years Later: Hero or Villain*, 39 Loy. U. Chi. L.J. 525 (2008)

Murthy, Dodderi Narshima Prabhakar et al., Product Reliability: Specification and Performance (2008)

Musger, Gottfried, *Zur Anwendung des PHG auf wirkungslose Produkte* [*Application of the Product Liability Act to Ineffective Products*], 1990 Wirtschaftsrechtliche Blätter 289 (Austria)

N. Am. Elec. Reliability Corp., Cyber Security — Critical Cyber Asset Identification, CIP-002-3 (2009), *available at* http://www.nerc.com/files/CIP-002-3.pdf

N. Am. Elec. Reliability Corp., Cyber Security — Electronic Security Perimeter(s), CIP-005-3 (2009), *available at* http://www.nerc.com/files/CIP-005-3.pdf

N. Am. Elec. Reliability Corp., Cyber Security — Incident Reporting and Response Planning, CIP-008-3, Requirement R1 (2009), *available at* http://www.nerc.com/files/CIP-008-3.pdf

N. Am. Elec. Reliability Corp., Cyber Security — Personnel & Training, CIP-004-3 (2009), *available at* http://www.nerc.com/files/CIP-004-3.pdf

N. Am. Elec. Reliability Corp., Cyber Security — Physical Security of Critical Cyber Assets, CIP-006-3c (2010), *available at* http://www.nerc.com/files/CIP-006-3c.pdf

N. Am. Elec. Reliability Corp., Cyber Security — Recovery Plans for Critical Cyber Assets, CIP-009-3 (2009), *available at* http://www.nerc.com/files/CIP-009-3.pdf

N. Am. Elec. Reliability Corp., Cyber Security — Security Management Controls, CIP-003-3 (2009), *available at* http://www.nerc.com/files/CIP-003-3.pdf

N. Am. Elec. Reliability Corp., Cyber Security — Systems Security Management, CIP-007-3 (2009), *available at* http://www.nerc.com/files/CIP-007-3.pdf

N. Am. Elec. Reliability Corp., Frequently Asked Questions (FAQs) for Cyber Security Standards: CIP-002-1 — Cyber Security — Critical Cyber Asset (2006), *available at* http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.pdf

N. Am. Elec. Reliability Corp., Frequently Asked Questions (FAQs) for Cyber Security Standards: CIP-005-1 — Cyber Security — Electronic Security (2006), *available at* http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-005-1_FAQs_20090217.pdf

N. Am. Elec. Reliability Corp., Frequently Asked Questions (FAQs) for Cyber Security Standards: CIP-007-1 — Cyber Security — Systems Security Management (2006), *available at* http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-007-1_FAQs_20090217.pdf

N. Am. Elec. Reliability Corp., Glossary of Terms Used in NERC Reliability Standards (2010), *available at* http://www.nerc.com/page.php?cid=2|20|283

N. Am. Elec. Reliability Corp., Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards, Appendix 4D to the Rules of Procedure (2010), *available at* http://www.nerc.com/files/ Appendix4D_TFE_Procedures_01212010.pdf

N. Atl. Treaty Org., NATO R&M Terminology Applicable to ARMPs, ARMP-7 (2008), *available at* http://www.nato.int/docu/stanag/armp7/armp-7_ed2-e.pdf

Nahra, Kirk J., *What Every Litigator Needs to Know About Privacy*, 902 PLI/Pat 277 (2007)

Nakashima, Ellen, *War game reveals U.S. lacks cyber-crisis skills*, Wash. Post, Feb. 17, 2010, at A3, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/16/ AR2010021605762.html

Naraine, Ryan, *Malware found in Lenovo software package*, ZDNet, Nov. 19, 2008, http://www.zdnet.com/blog/security/malware-found-in-lenovo-software-package/2203

Nat'l Acad. of Eng'g, Critical Information Infrastructure Protection and the Law: An Overview of Key Issues (Stewart D. Personick & Cynthia A. Patterson eds., 2003)

Nat'l Computer Sec. Ctr., Trusted Network Interpretation, NCSC-TG-005 (1987) (also known as the "Red Book"), *available at* http://csrc.nist.gov/publications/secpubs/ rainbow/tg005.txt

Nat'l Inst. of Standards & Tech., An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12 (1995), *available at* http://csrc.nist.gov/ publications/nistpubs/800-12/handbook.pdf

Nat'l Inst. of Standards & Tech., An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)

SECURITY RULE, SPECIAL PUBLICATION 800-66 REV. 1 (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

NAT'L INST. OF STANDARDS & TECH., GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING, SPECIAL PUBLICATION 800-83 (2005), *available at* http://csrc.nist.gov/ publications/nistpubs/800-83/SP800-83.pdf

NAT'L INST. OF STANDARDS & TECH., GUIDE TO SSL VPNS, SPECIAL PUBLICATION 800-113 (2008)

NAT'L INST. OF STANDARDS & TECH., GUIDELINES FOR MEDIA SANITIZATION, SPECIAL PUBLICATION 800-88 (2006), *available at* http://csrc.nist.gov/publications/nistpubs/800-88/ NISTSP800-88_rev1.pdf

NAT'L INST. OF STANDARDS & TECH., GUIDELINES FOR THE SELECTION AND USE OF TRANSPORT LAYER SECURITY (TLS) IMPLEMENTATIONS, SPECIAL PUBLICATIONS 800-52 (2005)

NAT'L INST. OF STANDARDS & TECH., MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 200 (2006), *available at* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NAT'L INST. OF STANDARDS & TECH., PERFORMANCE MEASUREMENT GUIDE FOR INFORMATION SECURITY, SPECIAL PUBLICATION 800-55 REV. 1 (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

NAT'L INST. OF STANDARDS & TECH., RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, SPECIAL PUBLICATION 800-53 REV. 3, (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

Nat'l Inst. of Standards & Tech., Recommended Security Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 3 (2009), *available at* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

Nat'l Inst. of Standards & Tech., Risk Management Guide for Information Technology Systems, Special Publication 800-30 (2002), *available at* http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Nat'l Inst. of Standards & Tech., Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140—2 (2001)

Nat'l Inst. of Standards & Tech., Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publication 199 (2004), *available at* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Nat'l Inst. of Standards & Tech., The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 (Draft) (2011), *available at* http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Nat'l Inst. of Standards & Tech., Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, Special Publication 800-60, Volume I, Revision 1 (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

Nat'l Inst. of Standards & Tech., Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, NIST Special Publication 800-60, Volume II, Revision 1 (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf

Nat'l Research Council, Cybersecurity Today and Tomorrow: Pay Now or Pay Later (2002)

Nat'l Research Council, Trust in Cyberspace (Fred B. Schneider ed., 1999)

Nat'l Sec. Agency, Controlled Access Protection Profile, Version 1.d (1999), *available at* http://www.niap-ccevs.org/cc-scheme/pp/PP_OS_CA_V1.d.pdf

Ng, James, Cisco Systems, Extensions to BGP to Support Secure Origin BGP (soBGP) (Apr. 2004), http://tools.ietf.org/html/draft-ng-sobgp-bgp-extensions-02

Nicastro, Felicia M., *Security Patch Management: The Process, in* Information Security Management Handbook 185 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Nielsen, Claus Kastberg et al., Study on the Economic Impact of the Electronic Commerce Directive (2007), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/ecd/%20final%20report_070907.pdf

Nimmer, Raymond T., 2 Information Law (2010)

Nissenbaum, Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life (2010)

Nolan, Patrick, *Unusable, Unreadable, or Indecipherable? No Breach reporting required*, SANS Internet Storm Center, May 9, 2009, http://isc.sans.org/diary.html?storyid=6364

Northcutt, Stephen & Novak, Judy, Network Intrusion Detection (3d ed. 2002)

Northcutt, Stephen et al., Inside Network Perimeter Security (2d ed. 2005)

Number Resource Org., Free Pool of IPv4 Address Space Depleted (Feb. 3, 2011), http://www.nro.net/news/ipv4-free-pool-depleted

O'Reilly, James T., 1 Food and Drug Administration (3rd ed. 2010)

O'Rourke, Maureen A., *An Essay on the Challenges of Drafting a Uniform Law of Software Contracting*, 10 Lewis & Clark L. Rev. 925 (2006)

Odlyzko, Andrew, *Privacy, Economics, and Price Discrimination on the Internet, in* Economics of Information Security 187 (L. Jean Camp & Stephen Lewis eds., 2004)

Office of Mgmt. & Budget, Executive Office of the President, Fiscal Year 2008 Report to Congress on Implementation of The Federal Information Security Management Act of 2002 (2009), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/reports/fy2008_fisma.pdf

Office of Mgmt. & Budget, Executive Office of the President, Fiscal Year 2009 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002 (2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf

Office of Mgmt. & Budget, Executive Office of the President, OMB Memorandum M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

Office of Mgmt. & Budget, Executive Office of the President, OMB Memorandum M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (2009)

OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (2007)

OFFICE OF TECHNOLOGY ASSESSMENT, COMPUTER-BASED NATIONAL INFORMATION SYSTEMS: TECHNOLOGY AND PUBLIC POLICY ISSUES (1981)

OGGERINO, CHRIS, HIGH AVAILABILITY NETWORK FUNDAMENTALS (2001)

Oppel, Richard A. Jr. & Sorkin, Andrew Ross, *Enron Admits to Overstating Profits by About $600 Million*, N.Y. TIMES, Nov. 9, 2001, at C1, *available at* http://www.nytimes.com/2001/11/09/business/enron-admits-to-overstating-profits-by-about-600-million.html

Orcutt, John L., *The Case Against Exempting Smaller Reporting Companies from Sarbanes-Oxley Section 404: Why Market-Based Solutions Are Likely to Harm Ordinary Investors*, 14 FORDHAM J. CORP. & FIN. L. 325 (2009)

Paetkau, Tyler & Torabian-Bashardoust, Roxanne, *California Deals with ID Theft: The Promise and the Problems*, BUS. L. TODAY, May-June 2004, at 37

Palmer, Charles C., *Can We Win the Security Game?*, 2 IEEE SECURITY & PRIVACY 10 (2004)

PANNENBECKER, ARND, MÜNCHENER ANWALTSHANDBUCH MEDIZINRECHT [MUNICH ATTORNEY HANDBOOK MEDICAL LAW] (Michael Terbille ed., 2009)

PARKER, DONN B., FIGHTING COMPUTER CRIME: A NEW FRAMEWORK FOR PROTECTING INFORMATION (1998)

Parker, Jerry & Grasmick, Harold G., *Linking Actual and Perceived Certainty of Punishment: An Exploratory Study of an Untested Proposition in Deterrence Theory*, 17 CRIMINOLOGY 366 (1979)

Paternoster, Raymond, *Assessments of Risk and Behavioral Experience: An Exploratory Study of Change*, 23 CRIMINOLOGY 417 (1985)

Paya, Cem, *Quasi-Secrets: The Nature of Financial Information and Its Implications for Data Security, in* HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 121 (Andrea M. Matwyshyn ed., 2009)

PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES, VERSION 2.0 (2010), *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

PELTIER, THOMAS R., INFORMATION SECURITY RISK ANALYSIS (2d ed. 2005)

Perera, David, *OMB gives DHS new powers under revised FISMA guidance*, FIERCEGOVERNMENTIT, Apr. 21, 2010, http://www.fiercegovernmentit.com/story/omb-gives-dhs-new-powers-under-revised-fisma-guidance/2010-04-21

Perlman, Daniel T., Notes and Comments, *Who Pays the Price of Computer Software Failure?*, 24 RUTGERS COMPUTER & TECH. L.J. 383 (1998)

PESCATORE, JOHN, GARTNER, HIGH-PROFILE THEFTS SHOW INSIDERS DO THE MOST DAMAGE, FT-18-9417 (2002), *available at* http://www.gartner.com/resources/111700/111710/111710.pdf

Phillips, Douglas E., *When Software Fails: Emerging Standards of Vendor Liability Under the Uniform Commercial Code*, 50 BUS. LAW. 151 (1994)

PHLIPS, LOUIS, THE ECONOMICS OF PRICE DISCRIMINATION (1983)

Picanso, Kathryn E., *Protecting Information Security Under A Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355 (2006)

Pichai, Sundar, Vice President, Google Inc., *Introducing the Google Chrome OS*, Official Google Blog, July 7, 2009, http://googleblog.blogspot.com/2009/07/introducing-google-chrome-os.html

Pilewski, Bonnie G. & Pilewski, Christopher A., *NERC Compliance: A Compliance Review, in* 3 Information Security Management Handbook 163 (Harold F. Tipton & Micki Krause eds., 6th ed. 2009)

Pinkney, Kevin R., *Putting Blame Where Blame is Due: Software Manufacturer And Customer Liability for Security-Related Software Failure*, 13 Alb. L.J. Sci. & Tech. 43 (2002)

Pinson, Chad, *New Legal Frontier: Mass Information Loss and Security Breach*, 11 SMU Sci. & Tech. L. Rev. 27 (2007)

Pinto, Timothy et al., *Liability of Online Publishers for User Generated Content: A European Perspective*, Comm. Law., Apr. 2010, at 5

Png, I.P.L. & Wang, Chen-yu, The Deterrent Effect of Enforcement Against Computer Hackers: Cross-Country Evidence (Sixth Workshop on the Economics of Information Security, Working Paper, 2007), *available at* http://weis2007.econinfosec.org/papers/77.pdf

Ponemon Inst., 2009 PCI DSS Compliance Survey (2009), *available at* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/PCI%20DSS%20Survey%20Key%20Findings%20FINAL4.pdf

Ponemon Inst., Business Risk of a Lost Laptop: A Study of IT Practitioners in the United States, United Kingdom, Germany, France, Mexico & Brazil (2009), *available* *at* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/The%20Business%20Risk%20of%20a%20Lost%20Laptop%20%28Global%29%20Final%204.pdf

PONEMON INST., NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION (2005), *available at* http://www.whitecase.com/files/FileControl/863d572d-cde3-4e33-903c-37eaba537060/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/Security_Breach_Survey%5B1%5D.pdf

Popescu, Alin C. et al., The Anatomy of a Leak: AS9121 or How We Learned to Start Worrying and Hate the Maximum Prefix Limits (May 15, 2005), http://www.nanog.org/meetings/nanog34/presentations/underwood.pdf

Posner, Richard A., *Theories of Economic Regulation*, 5 BELL J. ECON. & MGMT. SCI. 335 (1974)

POSTEL, J. & REYNOLDS, J., FILE TRANSFER PROTOCOL (FTP), RFC 959 (1985), ftp://ftp.rfc-editor.org/in-notes/rfc959.txt

POSTEL, J., INTERNET CONTROL MESSAGE PROTOCOL, RFC 792 (1981), ftp://ftp.rfc-editor.org/in-notes/rfc792.txt

POSTEL, J., INTERNET PROTOCOL—DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 791 (1981), ftp://ftp.rfc-editor.org/in-notes/rfc791.txt

POSTEL, J., TRANSMISSION CONTROL PROTOCOL, RFC 793 (1981), ftp://ftp.rfc-editor.org/in-notes/rfc793.txt

POSTEL, J., USER DATAGRAM PROTOCOL, RFC 768 (1980), ftp://ftp.rfc-editor.org/in-notes/rfc768.txt

Poulsen, Kevin, *Breakable*, SECURITYFOCUS, Jan. 16, 2002, http://www.securityfocus.com/news/309

Poulsen, Kevin, *California disclosure law has national reach*, SECURITYFOCUS, Jan. 6, 2003, http://www.securityfocus.com/news/1984

Poulsen, Kevin, *Thwarted Linux backdoor hints at smarter hacks*, SECURITYFOCUS, Nov. 6, 2003, http://www.securityfocus.com/news/7388

Power, Richard, *Corporate Espionage: Tomorrow Arrived Yesterday*, CSOONLINE.COM, Feb. 26, 2010, http://www.csoonline.com/article/558021/corporate-espionage-tomorrow-arrived-yesterday

Prentice, Robert, *Sarbanes-Oxley: The Evidence Regarding the Impact of Sox 404*, 29 CARDOZO L. REV. 703 (2007)

Preston, Ethan & Turner, Paul, *The Global Rise of A Duty to Disclose Information Security Breaches*, 22 J. MARSHALL J. COMPUTER & INFO. L. 457 (2004)

Price, Sean M., *Operations Security, in* OFFICIAL (ISC)^2 GUIDE TO THE CISSP CBK 633 (Harold F. Tipton ed., 2007)

PRIDGEN, MARY DEE, CONSUMER PROTECTION AND THE LAW (2010)

Prosser, William L., *Privacy*, 48 CAL. L. REV. 383 (1960)

PUB. CO. ACCOUNTING OVERSIGHT BD., AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A (2007), *available at* http://pcaobus.org/Rules/Rulemaking/Docket%20021/2007-06-12_Release_No_2007-005A.pdf

PUB. CO. ACCOUNTING OVERSIGHT BD., AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING PERFORMED IN CONJUNCTION WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 2, RELEASE NO. 2004-001 (2004)

PUB. CO. ACCOUNTING OVERSIGHT BD., AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS, AUDITING STANDARD NO. 5, RELEASE NO. 2007-005A (2007)

PURCELL, JAMES E., SECURITY CONTROL TYPES AND OPERATIONAL SECURITY (2007), http://www.giac.org/resources/whitepaper/operations/207.pdf

Rabin, Robert L., *Tort Recovery for Negligently Inflicted Economic Loss: A Reassessment,* 37 STAN. L. REV. 1513 (1985)

Rabkin, Michael A., *When Consumer Fraud Crosses the International Line: The Basis for Extraterritorial Jurisdiction Under the FTC Act*, 101 NW. U. L. REV. 293 (2007)

RAINSON, TARA ALEXANDRA, CONG. RESEARCH SERV., IDENTITY THEFT LAWS: STATE PENALTIES AND REMEDIES AND PENDING FEDERAL BILLS, CRS REPORT FOR CONGRESS RL34028 (2007), *available at* http://opencrs.com/document/RL34028/2007-08-06/download/1005/

RÅMAN, JARI, REGULATING SECURE SOFTWARE DEVELOPMENT (2006)

Ramasastry, Anita, *Web sites change prices based on customers' habits*, CNN.COM, June 24, 2005, http://edition.cnn.com/2005/LAW/06/24/ramasastry.website.prices/

RAMBØLL MANAGEMENT, ECONOMIC EVALUATION OF THE DATA PROTECTION DIRECTIVE 95/46/EC (2005), *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/economic_evaluation_en.pdf

RAMOS, MICHAEL J., HOW TO COMPLY WITH SARBANES-OXLEY SECTION 404: ASSESSING THE EFFECTIVENESS OF INTERNAL CONTROL (2008)

RAMSDELL, B. & TURNER, S., SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME) VERSION 3.2 MESSAGE SPECIFICATION, RFC 5751 (2010), ftp://ftp.rfc-editor.org/in-notes/rfc5751.txt

Rancher, Clinton W., Note, *More Art Than Science: The State-of-the-Art in Fraud Risk Assessment and Its Implications for Auditing Standard No. 5*, 6 GEO. J.L. & PUB. POL'Y 371 (2008)

Raul, Alan Charles et al., *Liability for Computer Glitches and Online Security Lapses*, 6 ELECTRONIC COM. & L. REP. 849 (2001)

RAYMOND, ERIC S., ET AL., THE NEW HACKER'S DICTIONARY (1996)

RAYMOND, ERIC S., THE CATHEDRAL & THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY (2001)

RAYMOND, ERIC STEVEN, THE ART OF UNIX PROGRAMMING (2003)

Reber, Greg, *PCI compliance falls short of assuring website security*, SEARCHSOFTWAREQUALITY.COM, Oct. 27, 2008, http://searchsoftwarequality.techtarget.com/news/column/0,294698,sid92_gci1335662,00.html

Recent Case, *Federal District Court Denies § 230 Immunity to Website That Solicits Illicit Content - FTC v. Accusearch, Inc.*, 121 HARV. L. REV. 2246 (2008)

Redhead, C. Stephen, *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations*, *in* THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA): OVERVIEW AND ANALYSES 69 (Susan Boriotti & Donna Dennis eds., 2004)

Reed, Chris & Welterveden, Alison, *Liability, in* COMPUTER LAW 87 (Chris Reed & John Angel eds., 4th ed. 2000)

REESE, GEORGE, CLOUD APPLICATION ARCHITECTURES: BUILDING APPLICATIONS AND INFRASTRUCTURE IN THE CLOUD (2009)

Regan, Priscilla M., *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103 (2009)

REGAN, PRISCILLA M., LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995)

Reidenberg, Joel R., *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995)

REKHTER, Y. & GROSS, P., APPLICATION OF THE BORDER GATEWAY PROTOCOL IN THE INTERNET, RFC 1772 (1995), ftp://ftp.rfc-editor.org/in-notes/rfc1772.txt

REKHTER, Y. ET AL., A BORDER GATEWAY PROTOCOL 4 (BGP-4), RFC 4271 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4271.txt

REPGEN, TILMAN, KEIN ABSCHIED VON DER PRIVATAUTONOMIE: DIE FUNKTION ZWINGENDEN RECHTS IN DER VERBRAUCHSGÜTERKAUFRICHTLINIE [NO FAREWELL TO PRIVATE AUTONOMY: THE ROLE OF *IUS COGENS* IN THE CONSUMER SALES DIRECTIVE] (2001)

RESCORLA, E., TRANSPORT LAYER SECURITY (TLS) RENEGOTIATION INDICATION EXTENSION, RFC 5746 (2010), ftp://ftp.rfc-editor.org/in-notes/rfc5746.txt

RESTATEMENT (SECOND) OF TORTS (1965)

RESTATEMENT (SECOND) OF TORTS (2009)

RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY (1998)

Retzer, Karin, *Data Breach Notification: The Changing Landscape in the EU*, 2 COMPUTER L. REV. INT'L 39 (2008) (F.R.G.)

Rice, David, Geekonomics: The Real Cost of Insecure Software (2008)

Rice, Denis T., *Increased Civil Litigation Over Privacy and Security Breaches*, 902 PLI/Pat 149 (2007)

RiskMetrics Group et al., Study on Monitoring and Enforcement Practices in Corporate Governance in the Member States (2009), *available at* http://ec.europa.eu/internal_market/company/docs/ecgforum/studies/comply-or-explain-090923_en.pdf

Rittinghouse, John W. & Ransome, James F., Cloud Computing: Implementation, Management, and Security (2010)

Robertson, Campbell & Kaufman, Leslie, *Size of Spill in Gulf of Mexico Is Larger Than Thought,* N.Y. Times, Apr. 29, 2010, at A14, *available at* http://www.nytimes.com/2010/04/29/us/29spill.html

Robinson, Neil et al, Review of the European Data Protection Directive (2009), *available at* http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf

Robinson, Shane W., Corporate Espionage 201 (2007), *available at* http://www.sans.org/reading_room/whitepapers/engineering/corporate-espionage-201_512

Rodau, Andrew, *Computer Software: Does Article 2 of the Uniform Commercial Code Apply?*, 35 Emory L.J. 853 (1986)

Rode, Lilia, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 Hous. L. Rev. 1597 (2007)

Rogers, Marcus K., *Legal, Regulations, Compliance and Investigations, in* Official (ISC)^2 Guide to the CISSP CBK 683 (Harold F. Tipton ed., 2007)

Romano, Roberta, *Does the Sarbanes-Oxley Act Have A Future?*, 26 YALE J. ON REG. 229 (2009)

ROMANOSKY, SASHA ET AL., DO DATA BREACH DISCLOSURE LAWS REDUCE IDENTITY THEFT? (SEVENTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, WORKING PAPER, 2008), *available at* http://weis2008.econinfosec.org/papers/Romanosky.pdf

Romero, Simon & Berenson, Alex, *WorldCom Says It Hid Expenses, Inflating Cash Flow $3.8 Billion*, N.Y. TIMES, June 26, 2002, at A1

ROSEN, LAWRENCE, OPEN SOURCE LICENSING: SOFTWARE FREEDOM AND INTELLECTUAL PROPERTY LAW (2004)

ROSENBERG, J. ET AL., SIP: SESSION INITIATION PROTOCOL, RFC 3261 (2002), ftp://ftp.rfc-editor.org/in-notes/rfc3261.txt

Rowland, Diane, *Liability for Defective Software*, 22 CAMBRIAN L. REV. 78 (1991)

Ruder, David S. et al., *The SEC at 70: The Securities and Exchange Commission's Pre-and Post-Enron Responses to Corporate Financial Fraud: An Analysis and Evaluation*, 80 NOTRE DAME L. REV. 1103 (2005)

RUNDFUNK UND TELEKOM REGULIERUNGS-GMBH, 4 JAHRE SIGNATURGESETZ [4 YEARS SIGNATURE ACT] (2004), *available at* http://www.signatur.rtr.at/repository/rtr-report-20040116-de.pdf

RUSSEL, CHARLIE ET AL., MICROSOFT WINDOWS 2000 SERVER ADMINISTRATOR'S COMPANION (2d ed. 2003)

RUSSELL, TRAVIS, SIGNALING SYSTEM #7 (5th ed. 2006)

Rustad, Michael L. & Koenig, Thomas H., *Rebooting Cybertort Law*, 80 WASH. L. REV. 335 (2005)

Rustad, Michael L. & Koenig, Thomas H., *The Tort of Negligent Enablement of Cybercrime,* 20 BERKELEY TECH. L.J. 1553 (2005)

Rustad, Michael L., *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDIS. L.J. 63 (2001)

S. Comm. on Commerce, Science, and Transportation, *Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (2005)

S. Comm. on Commerce, Science, and Transportation, *Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (2005)

S. Comm. on Homeland Security and Governmental Affairs, *Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?: Hearing Before the Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the S. Comm. on Homeland Security and Governmental Affairs*, 110th Cong. (2008)

Salter, Jessica, *Camera sold on eBay contained MI6 files*, DAILY TELEGRAPH (U.K.), Sept. 30, 2008, available at http://www.telegraph.co.uk/news/uknews/3107003/Camera-sold-on-eBay-contained-MI6-files.html

Saltzer, Jerome H. & Schroeder, Michael D., *The Protection of Information in Computer Systems*, 63 PROCEEDINGS OF THE IEEE 1278 (1975)

Saltzer, Jerry H. et al., *End-To-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYS. 277 (1984)

Sanchidrian, Guido, *EuroSOX is not US-SOX*, Symantec Connect, Mar. 19, 2009, *available at* http://www.symantec.com/connect/articles/eurosox-not-us-sox

Sand, Stephen L., *Validity, Construction, and Application of Computer Software Licensing Agreements*, 38 A.L.R. 5th 1 (1996)

SANS Inst. & MITRE Corp., 2010 CWE/SANS Top 25 Most Dangerous Software Errors (2010), *available at* http://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.pdf

SANS Inst., *Cyber Attack Simulation Underscores Areas of Policy Weakness*, SANS NewsBites (SANS Institute, Bethesda, Md.), Feb. 19, 2010, http://www.sans.org/newsletters/newsbites/newsbites.php?vol=12&issue=14#sID201

SANS Inst., Press Release, New Top 25 Software Errors Opens Door to Shift Liability for Faulty Code from Buyers to Developers (Feb. 16, 2010), *available at* http://www.sans.org/top25-software-errors/press-release.php

Sartor, Giovanni et al., *The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*, 18 Int'l J.L. & Info. Tech. 356 (2010)

Sauer, Jennifer H. & Walters, Neal, Am. Ass'n of Retired Persons, Security Freeze Legislation: Awareness and Incidence of Placement Among Consumers 18+ in Seven States (2007), *available at* http://assets.aarp.org/rgcenter/consume/freeze_leg.pdf

Savage, Sam L., The Flaw of Averages: Why We Underestimate Risk in the Face of Uncertainty (2009)

Saxby, Stephen J., *Liability for On-line Data Bank Services in the United Kingdom*, *in* LIABILITY FOR ON-LINE DATA BANK SERVICES IN THE EUROPEAN COMMUNITY 321 (Ulrich Sieber ed., 1992)

SCHAAR, PETER, DAS ENDE DER PRIVATSPHÄRE: DER WEG IN DIE ÜBERWACHUNGSGESELLSCHAFT [THE END OF PRIVACY: THE WAY INTO THE SURVEILLANCE SOCIETY] (2007)

SCHILLER, CRAIG A. ET AL., BOTNETS: THE KILLER WEB APP (2007)

SCHLICK, AUSTIN, GENERAL COUNSEL AT THE FCC, A THIRD-WAY LEGAL FRAMEWORK FOR ADDRESSING THE COMCAST DILEMMA (2010), *available at* http://www.fcc.gov/Daily_ Releases/Daily_Business/2010/db0506/DOC-297945A1.pdf

SCHMIDT-SALZER, JOACHIM, 1 KOMMENTAR EG-RICHTLINIE PRODUKTHAFTUNG [1 COMMENTARY EC DIRECTIVE PRODUCT LIABILITY] (1986)

Schneider, Jochen, *Die EG-Richtlinie zum Datenschutz* [*The EC Directive About Data Protection*], 1993 COMPUTER UND RECHT 35 (F.R.G.)

SCHNEIER, BRUCE, APPLIED CRYPTOGRAPHY (2d ed. 1996)

SCHNEIER, BRUCE, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD (2006)

Schneier, Bruce, *Beyond Security Theater*, NEW INTERNATIONALIST, Nov. 2009, at 10, *available at* http://www.schneier.com/essay-292.html

Schneier, Bruce, *BitArmor's No-Breach Guarantee*, SCHNEIER ON SECURITY, Jan. 23, 2009, http://www.schneier.com/blog/archives/2009/01/bitarmors_no-br.html

Schneier, Bruce, *Blaster and the great blackout*, SALON.COM, Dec. 16, 2003, http://dir.salon.com/story/tech/feature/2003/12/16/blaster_security/index.html

Schneier, Bruce, *Hacking the Business Climate for Network Security*, IEEE COMPUTER, Apr. 2004, at 87, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 151 (2008)

Schneier, Bruce, *How Security Companies Sucker Us With Lemons*, WIRED, Apr. 19, 2007, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2007/04/securitymatters_0419 *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 163 (2008)

Schneier, Bruce, *Information Security and Externalities*, ENISA Q. REV. (European Network & Info. Sec. Agency, Heraklion, Greece), Jan. 2007, at 3, *available at* http://www.enisa.europa.eu/publications/eqr/issues/eqr-q4-2006-vol.-2-no.-4/at_download/issue

Schneier, Bruce, *Is two-factor authentication too little, too late? It's not enough*, NETWORK WORLD, Apr. 4, 2005, http://www.networkworld.com/columnists/2005/040405faceoff-counterpane.html

Schneier, Bruce, *Make Vendors Liable for Bugs*, WIRED, June 6, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/06/71032, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 147 (2008)

Schneier, Bruce, *Mitigating Identity Theft*, CNET.COM, Apr. 14, 2005, http://news.cnet.com/Mitigating-identity-theft/2010-1071_3-5669408.html *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 205 (2008)

SCHNEIER, BRUCE, SCHNEIER ON SECURITY (2008)

SCHNEIER, BRUCE, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD (2000)

Schneier, Bruce, *The Anti-ID-Theft Bill That Isn't*, WIRED, Apr. 20, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/04/70690 *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 37 (2008)

Schneier, Bruce, *The Non-Security of Secrecy*, COMMUNICATIONS OF THE ACM, Oct. 2004, at 120, *available at* http://www.schneier.com/essay-056.html

Schneier, Bruce, *The Psychology of Security*, 2008 AFRICACRYPT 50

Schneier, Bruce, *Why Data Mining Won't Stop Terror*, WIRED, Mar. 9, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/03/70357, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 9 (2008)

SCHULTZ, E. EUGENE & SHUMWAY, RUSSELL, INCIDENT RESPONSE: A STRATEGIC GUIDE TO HANDLING SYSTEM AND NETWORK SECURITY BREACHES (2001)

SCHULZRINNE, H. ET AL., RTP: A TRANSPORT PROTOCOL FOR REAL-TIME APPLICATIONS, RFC 3550 (2003), ftp://ftp.rfc-editor.org/in-notes/rfc3550.txt

Schwartz, Paul M. & Janger, Edward J., *Notification of Data Security Breaches,* 105 MICH. L. REV. 913 (2007)

SCHWARZE, JÜRGEN, EUROPEAN ADMINISTRATIVE LAW (2006)

SCIENCE AND TECHNOLOGY COMMITTEE, PERSONAL INTERNET SECURITY VOLUME I: REPORT, 2006-7, H.L. 165–I, *available at* http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf

Scott, Michael D., *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425 (2008)

SEALED ET AL., STUDY ON CROSS-BORDER INTEROPERABILITY OF ESIGNATURES (CROBIES), NOTE ON THE "ALGO PAPER" ISSUE (2010), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.3.pdf

SEALED ET AL., STUDY ON CROSS-BORDER INTEROPERABILITY OF ESIGNATURES (CROBIES), COMMON SUPERVISION MODEL OF PRACTICES OF CERTIFICATION SERVICE PROVIDERS ISSUING QUALIFIED CERTIFICATES (2010), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd1.pdf

SEALED ET AL., STUDY ON CROSS-BORDER INTEROPERABILITY OF ESIGNATURES (CROBIES), FRAMEWORK FOR SECURE SIGNATURE CREATION DEVICES CROSS-BORDER RECOGNITION (2010), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd4.pdf

SEALED ET AL., STUDY ON THE STANDARDIZATION ASPECTS OF ESIGNATURE (2007), *available at* http://ec.europa.eu/information_society/policy/esignature/docs/standardisation/report_esign_standard.pdf

SEC. & EXCH. COMM'N, DIV. OF CORPORATION FINANCE & OFFICE OF THE CHIEF ACCOUNTANT, STAFF STATEMENT ON MANAGEMENT'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING (2005), *available at* http://sec.gov/info/accountants/stafficreporting.pdf

SEC. & EXCH. COMM'N, OFFICE OF ECONOMIC ANALYSIS, STUDY OF THE SARBANES-OXLEY ACT OF 2002 SECTION 404 INTERNAL CONTROL OVER FINANCIAL REPORTING REQUIREMENTS (2009), *available at* http://www.sec.gov/news/studies/2009/sox-404_study.pdf

SecureWorks, Inc., *PCI Update: Compliant Does Not Mean Secure*, SECUREWORKS' ON THE RADAR NEWSLETTER (SecureWorks, Inc., Ga.), Mar. 2009, http://www.secureworks.com/research/newsletter/2009/03/#pci

Segal, Donald E., *New Enforcement Initiatives—An Industry View*, 47 FOOD DRUG COSM. L.J. 421 (1992)

Selman, Jeffrey C. & Chen, Christopher S., *Steering the Titanic Clear of the Iceberg: Saving the Sale of Software From the Perils of Warranties*, 31 U.S.F. L. REV. 531 (1997)

SENIOR OFFICIALS GROUP INFORMATION SYSTEMS SECURITY, MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES, VERSION 3.0 (2010), *available at* http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/media/formal-docs/mra.pdf

SERWIN, ANDREW B., INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE (2009)

SERWIN, ANDREW B., INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL, STATE AND INTERNATIONAL LAW (2009)

Shafton, William R., *Complex Litigation in California and Beyond: California's Uncommon Common Law Class Action Litigation*, 41 LOY. L.A. L. REV. 783 (2008)

Shah, Pratik A., *The Uniform Computer Information Transactions Act*, 15 BERKELEY TECH. L.J. 85 (2000)

Shakespeare, Catherine, *Sarbanes-Oxley Act of 2002 Five Years on: What Have We Learned?*, 3 J. BUS. & TECH. L. 333 (2008)

SHAPIRO, CARL & VARIAN, HAL R., INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1999)

SHOSTACK, ADAM & STEWART, ANDREW, THE NEW SCHOOL OF INFORMATION SECURITY (2008)

Shostack, Adam & Syverson, Paul, *What Price Privacy (and why identity theft is about neither identity nor theft), in* ECONOMICS OF INFORMATION SECURITY 129 (L. Jean Camp & Stephen Lewis eds., 2004)

SHOSTACK, ADAM, AVOIDING LIABILITY: AN ALTERNATIVE ROUTE TO MORE SECURE PRODUCTS (FOURTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, WORKING PAPER, 2005), *available at* http://infosecon.net/workshop/pdf/44.pdf

Shull, Bernard, *Banking, commerce and competition under the Gramm-Leach-Bliley Act*, 47 ANTITRUST BULL. 25 (2002)

Silvers, Robert, *Rethinking FISMA and Federal Information Security Policy,* 81 N.Y.U. L. REV. 1844 (2006)

Simkin, M. V. & Roychowdhury, V. P., *Theory of Aces: Fame by Chance or Merit?*, 30 J. OF MATHEMATICAL SOC. 33 (2006)

Singh, Ritu, *Two-Factor Authentication: A Solution to Times Past or Present? The Debate Surrounding the Gramm-Leach-Bliley Security Safeguards Rule and the Methods of Risk Assessment and Compliance*, 2 I/S: J. L. & POL'Y FOR INFO. SOC'Y 761 (2006)

Skinner, Timothy H., *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet A Suitable Template For National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1 (2003), *available at* http://jolt.richmond.edu/v10i1/article1.pdf

Skoudis, Ed, *Hacker Attacks and Defenses, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 965 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Skoudis, Ed, *Hacker Tools and Techniques, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 935 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Slaughter-Defoe, Diana T. & Wang, Zhenlin, *Information Security of Children's Data, in* HARBORING DATA: INFORMATION SECURITY LAW AND THE CORPORATION 145 (Andrea M. Matwyshyn ed., 2009)

Smedinghoff, Thomas J. & Wu, Stephen S., *State Security Laws And Regulations—The New Deal*, 969 PLI/PAT 365 (2009)

Smedinghoff, Thomas J., *Defining the Legal Standard for Information Security: What Does "Reasonable" Security Really Mean?*, *in* SECURING PRIVACY IN THE INTERNET AGE 19 (Anupam Chander et al. eds., 2008)

SMEDINGHOFF, THOMAS J., INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE (2008)

Smedinghoff, Thomas J., *It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law*, 16 MICH. ST. J. INT'L L. 1 (2007)

Smith, Christopher, *The Magnuson-Moss Warranty Act: Turning The Tables on Caveat Emptor*, 13 CAL. WESTERN L. REV. 391 (1977)

SMITH, GRAHAM J.H., INTERNET LAW AND REGULATION (4th ed. 2007)

Smith, Graham, *Online Intermediary Liability,* CYBERSPACE LAW., Apr. 2009, at 19

SODTALBERS, AXEL, SOFTWAREHAFTUNG IM INTERNET [SOFTWARE LIABILITY ON THE INTERNET] (2006)

Solove, Daniel J., *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003)

SOLOVE, DANIEL J., INFORMATION PRIVACY LAW (2008)

SOLOVE, DANIEL J., THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004)

Solove, Daniel J., *The New Vulnerability: Data Security and Personal Information, in* SECURING PRIVACY IN THE INTERNET AGE 111 (Anupam Chander et al. eds., 2008)

SOLOVE, DANIEL J., UNDERSTANDING PRIVACY (2008)

SOMMER, PETER & BROWN, IAN, ORG. FOR ECON. CO-OPERATION AND DEV., REDUCING SYSTEMIC CYBERSECURITY RISK, IFP/WKP/FGS(2011)3 (2011), *available at* http://www.oecd.org/dataoecd/3/42/46894657.pdf

Songini, Marc L., *Retailers fume over PCI security rules*, COMPUTERWORLD, June 7, 2007, http://www.computerworld.com/s/article/9023998/Retailers_fume_over_PCI_security_rules

SourceForge, Sourceforge.net attack (Jan. 27, 2011), http://sourceforge.net/blog/sourceforge-net-attack/

Spears, Janine L., *How Has Sarbanes-Oxley Compliance Affected Information Security?,* 6 ISACA J. 33 (2009), *available at* http://www.isaca.org/Journal/Past-Issues/2009/Volume-6/Pages/How-Has-Sarbanes-Oxley-Compliance-Affected-Information-Security-1.aspx

SPINDLER, GERALD ET AL., VERANTWORTLICHKEITEN VON IT-HERSTELLERN, NUTZERN UND INTERMEDIÄREN [RESPONSIBILITIES OF IT MANUFACTURERS, USERS, AND INTERMEDIARIES] (2007), *available at* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf?__blob=publicationFile

SPURGEON, CHARLES E., ETHERNET: THE DEFINITIVE GUIDE (2000)

Stanek, Steve, *Auditing Cryptography: Assessing System Security, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1023 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Stern, Christopher, *FCC Cuts Public Line To Phone Outage Data*, WASH. POST, Aug. 28, 2004, at E01

Stevens, Gina Marie & Rainson, Tara Alexandra, *Data Security: Protecting the Privacy of Phone Records*, 887 PLI/PAT 337 (2006)

STEVENS, GINA MARIE, CONG. RESEARCH SERV., DATA SECURITY: FEDERAL LEGISLATIVE APPROACHES, CRS REPORT FOR CONGRESS RL33273 (2007), *available at* http://epic.org/privacy/idtheft/RL33273.pdf

STEVENS, GINA, CONG. RESEARCH SERV., FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS, CRS REPORT FOR CONGRESS RL34120 (2010), *available at* http://opencrs.com/document/RL34120/2010-01-28/download/1013

STEVENS, MARC ET AL., CHOSEN-PREFIX COLLISIONS FOR MD5 AND APPLICATIONS (2009), *available at* https://documents.epfl.ch/users/l/le/lenstra/public/papers/lat.pdf

STEVENS, MARC ET AL., VULNERABILITY OF SOFTWARE INTEGRITY AND CODE SIGNING APPLICATIONS TO CHOSEN-PREFIX COLLISIONS FOR MD5 (2007), *available at* http://www.win.tue.nl/hashclash/SoftIntCodeSign/

STEVENS, W. RICHARD, TCP/IP ILLUSTRATED, VOLUME 1: THE PROTOCOLS (1994)

Stigler, George J., *The Theory of Economic Regulation*, 2 BELL J. ECON. & MGMT. SCI. 3 (1971)

Storr, Stefan, *Grundsätze des Verwaltungsverfahrens aus gemeinschaftsrechtlicher Sicht* [*Principles of the Administrative Procedure from a Community Law Perspective*], *in* ABGABEVERFAHRENSRECHT UND GEMEINSCHAFTSRECHT [PUBLIC CHARGES PROCEDURAL LAW AND COMMUNITY LAW] 13 (Michael Holoubek & Michael Lang eds., 2006)

Stout, David & Zeller, Tom, *Vast Data Cache About Veterans Is Stolen*, N.Y. TIMES, May 23, 2006, *available at* http://www.nytimes.com/2006/05/23/washington/23identity.html

Strachan, Jane, *Cybersecurity Obligations*, 20 MAINE B. J. 90 (2005)

STUTTARD, DAFYDD & PINTO, MARCUS, THE WEB APPLICATION HACKER'S HANDBOOK: DISCOVERING AND EXPLOITING SECURITY FLAWS (2008)

Sullivan, Bob, *Why cell phone outage reports are secret*, MSNBC.COM, Dec. 15, 2006, http://redtape.msnbc.com/2006/12/why_cell_phone_.html

Sunstein, Cass R., *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613 (1999)

SYNOVATE, FEDERAL TRADE COMM'N – 2006 IDENTITY THEFT SURVEY REPORT (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

SYVERSON, PAUL, THE PARADOXICAL VALUE OF PRIVACY (SECOND WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, WORKING PAPER, 2003), *available at* http://www.cpppe.umd.edu/rhsmith3/papers/Final_session3_syverson.pdf

TAEGER, JÜRGEN, AUßERVERTRAGLICHE HAFTUNG FÜR FEHLERHAFTE COMPUTERPROGRAMME [NON-CONTRACTUAL LIABILITY FOR DEFECTIVE COMPUTER PROGRAMS] (1995)

Taeger, Jürgen, *Produkt- und Produzentenhaftung bei Schäden durch fehlerhafte Computerporgramme* [*Product and Producer Liability for Damages Caused by Faulty Computer Programs*], 1996 COMPUTER UND RECHT 257 (F.R.G.)

TALEB, NASSIM NICHOLAS, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE (2007)

TASCHNER, HANS CLAUDIUS & FRIETSCH, EDWIN, PRODUKTHAFTUNGSGESETZ UND EG-PRODUKTHAFTUNGSRICHTLINIE [PRODUCT LIABILITY ACT AND EC PRODUCT LIABILITY DIRECTIVE] (2d ed. 1990)

TAYLOR, LAURA, FISMA CERTIFICATION & ACCREDITATION HANDBOOK (2007)

THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT—A STRATEGIC PLAN (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf

Thompson Publ'g Group, *Radiation Treatment Software Maker Signs Consent Decree*, FDA ENFORCEMENT MANUAL NEWSL. (Thompson Publishing Group, Tampa, Fla.), Oct. 2003

Tiller, James S., *Access Control*, *in* OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 93 (Harold F. Tipton ed., 2007)

Tipton, Harold F., *Types of Information Security Controls, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 1357 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Trachtman, Joel P., *Global Cyberterrorism, Jurisdication, and International Organization, in* THE LAW AND ECONOMICS OF CYBERSECURITY 259 (Mark F. Grady & Francesco Parisi eds., 2006)

TURNER, MICHAEL, TOWARDS A RATIONAL PERSONAL DATA BREACH NOTIFICATION REGIME (2006), *available at* http://perc.net/files/downloads/data_breach.pdf

TUROW, JOSEPH ET AL., UNIVERSITY OF PENNSYLVANIA, ANNENBERG PUBLIC POLICY CENTER, OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE (2005), *available at* http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/Turow_APPC_Report_WEB_FINAL.pdf

Tversky, Amos & Kahneman, Daniel, *Belief in the law of small numbers, in* JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES 23 (Daniel Kahneman et al. eds., 1982)

Tversky, Amos & Kahneman, Daniel, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124 (1974)

Tversky, Amos & Kahneman, Daniel, *Prospect Theory: An Analysis of Decision under Risk*, 47 ECONOMETRICA 263 (1979)

U.K. MINISTRY OF DEFENCE, MOD GUIDE TO R&M TERMINOLOGY USED IN REQUIREMENTS, MINISTRY OF DEFENCE DEFENCE STANDARD 00-49 (2008), *available at* http://www.dstan.mod.uk/standards/defstans/00/049/00000200.pdf

U.K. OFFICE OF GOVERNMENT COMMERCE, INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY V3 (2007)

U.S. DEP'T OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997), *available at* http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm

U.S. DEP'T OF DEF., GUIDE FOR ACHIEVING RELIABILITY, AVAILABILITY, AND MAINTAINABILITY (2005), *available at* http://www.acq.osd.mil/dte/docs/RAM_Guide_080305.pdf

U.S. Dep't of Interior, Press Release, Flow Rate Group Provides Preliminary Best Estimate Of Oil Flowing from BP Oil Well (May 27, 2010), *available at* http://www.doi.gov/news/pressreleases/Flow-Rate-Group-Provides-Preliminary-Best-Estimate-Of-Oil-Flowing-from-BP-Oil-Well.cfm

U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES (2007), *available at* http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf

U.S. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977), *available at* http://epic.org/privacy/ppsc1977report/

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2010 REPORT TO CONGRESS 243 (2010), *available at* http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf

Ullrich, Johannes, *FAQ To IPv4 Exhaustion*, SANS INTERNET STORM CENTER, Feb. 1, 2011, http://isc.sans.edu/diary.html?storyid=10342

United Press Int'l, *Virus strikes 15 million PCs*, UPI.COM, Jan. 26, 2009, http://www.upi.com/Top_News/2009/01/26/Virus-strikes-15-million-PCs/UPI-19421232924206/

US-CERT, MD5 vulnerable to collision attacks, Vulnerability Note VU#836068 (Dec. 31, 2008), http://www.kb.cert.org/vuls/id/836068

Valliere, Rick & Aplin, Donald G., *Identity Theft: TJX Settles Consumer Class Breach Claims; Bank Class Actions Against Retailer Continue*, 12 ELECTRONIC COM. & L. REP. 905 (2007)

VAN EETEN, MICHEL J.G. & BAUER, JOHANNES M., ORG. FOR ECON. CO-OPERATION AND DEV., ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES, DSTI/DOC(2008)1 (2008), *available at* http://www.oecd.org/dataoecd/53/17/40722462.pdf

van Oorschot, P. C. et al., *On interdomain routing security and pretty secure BGP (psBGP)*, ACM TRANSACTIONS ON INFO. AND SYSTEM SECURITY, July 2007, *available at* http://delivery.acm.org/10.1145/1270000/1266980/a11-oorschot.pdf?key1=1266980&key2=2309656921&coll=DL&dl=ACM&CFID=7524552&CFTOKEN=54618690

VAN SCHEWICK, BARBARA, INTERNET ARCHITECTURE AND INNOVATION (2010)

Vangelos, Michael, *Managing the Response to a Computer Security Incident, in* INFORMATION SECURITY MANAGEMENT HANDBOOK 2989 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

VANSTRAELEN, ANN ET AL., MAASTRICHT ACCOUNTING, AUDITING AND INFORMATION MANAGEMENT RESEARCH CENTER, EVALUATION OF THE DIFFERENCES BETWEEN INTERNATIONAL STANDARDS ON AUDITING (ISA) AND THE STANDARDS OF THE US PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB) (2009), *available at* http://ec.europa.eu/internal_market/auditing/docs/ias/evalstudy2009/report_en.pdf

VARIAN, HAL R. ET AL., THE ECONOMICS OF INFORMATION TECHNOLOGY: AN INTRODUCTION (2004)

Varian, Hal R., *Differential Pricing and Efficiency*, 1 FIRST MONDAY (1996), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/473/394

VARIAN, HAL R., INTERMEDIATE MICROECONOMICS: A MODERN APPROACH (7th ed. 2005)

Varian, Hal R., *Versioning Information Goods, in* INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL INFORMATION AND INTELLECTUAL PROPERTY 190 (Brian Kahin & Hal R. Varian eds., 2000)

Velichety, Swapna et al., *Company Perspectives on Business Value of IT Investments in Sarbanes-Oxley Compliance*, 1 ISACA J. 42 (2007), *available at* http://www.isaca.org/Journal/Past-Issues/2007/Volume-1/Pages/Company-Perspectives-on-Business-Value-of-IT-Investments-in-Sarbanes-Oxley-Compliance.aspx

VERBIEST, THIBAULT ET AL., STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES (2007), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/ecd/%20final%20report_070907.pdf

Verton, Dan, *Survey Finds Digital Divide Among Federal CISOs*, COMPUTERWORLD, Nov. 22, 2004, http://www.computerworld.com/s/article/print/97763/Survey_finds_digital_divide_among_federal_CISOs

VIEGA, JOHN & MCGRAW, GARY, BUILDING SECURE SOFTWARE: HOW TO AVOID SECURITY PROBLEMS THE RIGHT WAY (2001)

VIEGA, JOHN, THE MYTHS OF SECURITY: WHAT THE COMPUTER SECURITY INDUSTRY DOESN'T WANT YOU TO KNOW (2009)

Vijayan, Jaikumar, *Banks may soon require new online authentication steps*, COMPUTERWORLD, Jan. 25, 2011, http://www.computerworld.com/s/article/9206158/Banks_may_soon_require_new_online_authentication_steps?taxonomyId=82

VOGL, ROLAND, THE EU-U.S PRIVACY CONTROVERSY: A QUESTION OF LAW OR GOVERNANCE? (2000), *available at* http://sls-stage.stanford.edu/publications/dissertations_theses/diss/VoglRoland-tft2000.pdf

von Gravenreuth, Günter Freiherr, *Computerviren und Haftung des Arbeitnehmers* [*Computer Viruses and Employee Liability*], SICHERHEITS-BERATER, Apr. 1993, Supp., at 2 (F.R.G.)

von Westphalen, Friedrich Graf, *Das deutsche Produkthaftungsgesetz* [*The German Product Liability Act*], *in* 2 PRODUKTHAFTUNGSHANDBUCH [2 PRODUCT LIABILITY HANDBOOK] (Friedrich Graf von Westphalen ed., 1999)

Wachler, Andrew B. & Fehn, Amy K., *The HITECH Breach Notification Rules: Understanding the New Obligations*, HEALTH LAW., Oct. 2009, at 1

Wait, Patience, *Federal government earns a collective D+ on FISMA scorecard*, GOV'T COMPUTER NEWS, Mar. 16, 2006, http://gcn.com/articles/2006/03/16/federal-government-earns-a-collective-d-on-fisma-scorecard.aspx

Wan, Tao et al., *A selective introduction to border gateway protocol (BGP) security issues, in* ASPECTS OF NETWORK AND INFORMATION SECURITY 152 (Evangelos Kranakis et al. eds., 2008)

Wang, Ju An et al., *Security Metrics for Software Systems*, 47 ACM SOUTHEAST REGIONAL CONF. (2009)

WANG, XIAOYUN ET AL., COLLISIONS FOR HASH FUNCTIONS MD4, MD5, HAVAL-128 AND RIPEMD (2004), *available at* http://eprint.iacr.org/2004/199.pdf

Warren, Samuel D. & Brandeis, Louis D., *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)

Washkuch, Frank, *Is FISMA fixable?*, SC MAGAZINE, Sept. 1, 2007, http://www.scmagazineus.com/is-fisma-fixable/article/35617/

Weber, Tim, *Criminals 'may overwhelm the web,'* BBC NEWS, Jan. 25, 2007, http://news.bbc.co.uk/1/hi/business/6298641.stm

WEBSENSE SECURITY LABS, STATE OF INTERNET SECURITY, Q3 – Q4, 2009 (2010), *available at* https://www.websense.com/assets/reports/WSL_H2_2009.pdf

WELSER, RUDOLF & RABL, CHRISTIAN, PRODUKTHAFTUNGSGESETZ [PRODUCT LIABILITY ACT] (2d ed. 2004)

WESTFALL, LINDA, THE CERTIFIED SOFTWARE QUALITY ENGINEER HANDBOOK (2010)

WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

White, Anthony E., Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who is Going to Pay for It?*, 88 MARQ. L. REV. 847 (2005)

White, Daniel M., Note, *The Federal Information Security Management Act of 2002: A Potemkin Village*, 79 FORDHAM L. REV. 369 (2010)

White, Russ, Cisco Systems, *Securing BGP Through Secure Origin BGP*, INTERNET PROTOCOL J., Sept. 2003, at 15, *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/ipj_6-3.pdf

Wilson, Clay, *Cyber Crime, in* CYBERPOWER AND NATIONAL SECURITY 415 (Franklin D. Kramer et al. eds., 2009)

Wilson, James Q., *The Politics of Regulation, in* THE POLITICS OF REGULATION 370 (James Q. Wilson ed., 1980)

Winn, Jane K., *Are "Better" Security Breach Notification Laws Possible?,* 24 BERKELEY TECH. L.J. 1133 (2009)

Winn, Peter A., *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L. J. 617 (2002)

WITKIN, B.E., 5 SUMMARY OF CALIFORNIA LAW, Torts (10th ed. 2005)

WITKIN, B.E., 6 SUMMARY OF CALIFORNIA LAW, Torts (10th ed. 2005)

Wolf, Klaus, *Zur Anforderung eines internen Kontroll- und Risikomanagementsystems im Hinblick auf den (Konzern-) Rechnungslegungsprozess gemäß BilMoG* [*On the Requirement of an Internal Control and Risk Management System with Regard to the (Consolidated) Financial Reporting Process Pursuant to BilMoG*], 2009 DEUTSCHES STEUERRECHT 920

WORKING GROUP ON INTERNET GOVERNANCE, REPORT OF THE WORKING GROUP ON INTERNET GOVERNANCE (2005), *available at* http://www.wgig.org/docs/WGIGREPORT.pdf

WU, CHI CHI & DE ARMOND, ELISABETH, FAIR CREDIT REPORTING (6th ed. 2006)

Wu, Stephen, *California Health Care Data Protection Law Addresses Worker Snooping*, RSA CONFERENCE BLOG, Apr. 12, 2009, https://365.rsaconference.com/blogs/ediscovery/2009/04

Wuermeling, Ulrich U., *Harmonisation of European Union Privacy Law*, 14 J. MARSHALL J. COMPUTER & INFO. L. 411 (1996)

Würmeling, Ulrich, *Datenschutz für die Europäische Informationsgesellschaft* [*Data Protection for the European Information Society*], 1995 NEUEN JURISTISCHEN WOCHENSCHRIFT – COMPUTERREPORT 111 (F.R.G.)

Yoo, Christopher S., *Network Neutrality and the Economics of Congestion*, 95 GEO. L.J. 1847 (2006)

ZERRES, THOMAS, DIE BEDEUTUNG DER VERBRAUCHSGÜTERKAUFRICHTLINIE FÜR DIE EUROPÄISIERUNG DES VERTRAGSRECHTS [THE SIGNIFICANCE OF THE CONSUMER SALES DIRECTIVE FOR THE EUROPEANIZATION OF CONTRACT LAW] (2007)

Zetter, Kim, *Revealed: The Internet's Biggest Security Hole*, WIRED.COM, Aug. 26, 2008, http://www.wired.com/threatlevel/2008/08/revealed-the-in/

Zimet, Elihu & Barry, Charles L., *Military Service Overview, in* CYBERPOWER AND NATIONAL SECURITY 285 (Franklin D. Kramer et al. eds., 2009)

ZITTRAIN, JONATHAN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008)

Zollers, Frances E. et al., *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745 (2005)

ZWICKY, ELIZABETH D. ET AL., BUILDING INTERNET FIREWALLS (2d ed. 2000)

List of Abbreviations

In addition to the abbreviations provided by *The Bluebook*, this thesis uses the following abbreviations:

ALE	Annualized Loss Expectancy
ARRA	American Recovery and Reinvestment Act of 2009
AS	Auditing Standard
AS	Autonomous System
ASN	Autonomous System Number
ATM	automated teller machine
BGP	Border Gateway Protocol
BRD	Better Regulation Directive
C&A	certification and accreditation
ccTLD	country-code TLD
CDA	Communications Decency Act
CDPH	California Department of Public Health
CEO	Chief Executive Officer
CFAA	Computer Fraud and Abuse Act
CFO	Chief Financial Officer
CIIP	Critical Information Infrastructure Protection
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CLRA	Consumers Legal Remedies Act
COPPA	Children’s Online Privacy Protection Act
COTS	commercial off-the-shelf software
CPLR	New York Civil Practice Law and Rules
CPNI	customer proprietary network information
CRD	Citizens’ Rights Directive
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration

DDoS	distributed denial of service
DNS	Domain Name System
DoS	denial of service
DPO	Data Protection Official
DSL	Digital Subscriber Line
EAL	Evaluation Assurance Level
ENISA	European Network and Information Security Agency
ePHI	electronic PHI
ERO	Electric Reliability Organization
E-SIGN	Electronic Signatures in Global and National Commerce Act
ESP	Electronic Security Perimeter
EUDPD	Data Protection Directive
FACTA	Fair and Accurate Credit Transactions Act
FCC	Federal Communications Commission
FCRA	Fair Credit Reporting Act
FDA	Food and Drug Administration
FDIC	Federal Deposit Insurance Corporation
FERC	Federal Energy Regulatory Commission
FFDCA	Federal Food, Drug, and Cosmetic Act
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
gTLD	generic TLD
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HITECH Act	Health Information Technology for Economic and Clinical Health Act

HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	information and communication technology
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPRED	Intellectual Property Rights Enforcement Directive
ISAC	Information Sharing and Analysis Center
ISBNA	New York Information Security Breach and Notification Act
ISO	International Organization for Standardization
IT	information technology
MMWA	Magnuson-Moss Warranty Act
NCUA	National Credit Union Administration
NERC	North American Electric Reliability Corporation
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NPRM	Notice of Propose Rule Making
OCC	Office of the Comptroller of the Currency
OMB	Office of Management and Budget
OSS	open source software
OTS	Office of Thrift Supervision
PC	personal computer
PCAOB	Public Company Accounting Oversight Board
PCI	DSS PCI Data Security Standard
PCI	Payment Card Industry
PHI	protected health information
PHR	personal health record
PKI	Public Key Infrastructure

PSD	Payment Services Directive
PSP	Physical Security Perimeter
PSTN	public switched telephone network
SCADA	Supervisory Control and Data Acquisition
SEC	Securities and Exchange Commission
SMTP	Simple Mail Transfer Protocol
SOX	Sarbanes-Oxley Act
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSN	Social Security number
TCP	Transmission Control Protocol
TFE	Technical Feasibility Exception
TLD	top-level domain
TLS	Transport Layer Security
UCC	Uniform Commercial Code
UCITA	Uniform Computer Information Transactions Act
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VA	Veterans Affairs
VoIP	Voice over IP
XML	Extensible Markup Language
XSS	cross-site scripting