Stanford Technology Law Review

Social Media Privacy: A Dozen Myths and Facts

LOTHAR DETERMANN*

CITE AS: 2012 STAN. TECH. L. REV. 7
http://stlr.stanford.edu/pdf/determann-socialmediaprivacy.pdf

¶1 Social networks and media are one of the latest frontiers for lawyers, lawmakers, politicians, entrepreneurs and academics. No one seems to claim that social media is the *final* frontier[1] or even a particularly revolutionary frontier. After all, media and social networks have been around for thousands of years in one form or another. But, most are genuinely fascinated with the new opportunities, risks, and questions presented by the recent rapid rise of novel technology platforms that allow people all over the world to connect and communicate in new ways. Thus the usual games begin: innovators, early adopters, libertarians, and businesses assert that social media is not, should not, and cannot be regulated, as previously with cyberspace and virtual worlds. Concerned politicians, on the other hand, claim that social media is new, dangerous, and in dire need of regulation. Entrepreneurs explore new ways to monetize the new phenomena. All involved create buzzwords, hype, and myths to support their respective agendas. In this article, I am taking on twelve myths that frequently come up in such discussions, including at the 2012 Symposium of the Stanford Technology Law Review on "First Amendment Challenges in the Digital Age."[2]

MYTH 1: YOU HAVE PRIVACY RIGHTS AGAINST SOCIAL MEDIA COMPANIES

¶2 Expectations of data privacy and privacy rights tend to be grossly exaggerated these days.[3] Fact is that most constitutions and international human rights treaties do not explicitly recognize rights to privacy.[4] Even if you find privacy rights in constitutions, expressly or impliedly, constitutional rights

* Dr. iur habil, Privatdozent, teaches Data Privacy Law, E-Commerce Law and Computer Law at Freie Universität Berlin; University of California, Berkeley School of Law and Hastings College of the Law; and Stanford Law School; Partner, Baker & McKenzie LLP, San Francisco and Palo Alto, California. The author thanks his student Emmanuel Fua, J.D. Candidate Stanford Law School, 2012, for valuable research assistance and contributions.

[1] That has been claimed for space, *see Star Trek: The Original Series*, WIKIPEDIA, http://en.wikipedia.org/wiki/Star_Trek:_The_Original_Series (last visited Apr. 30, 2012), and quite a few other phenomena.

[2] *Symposium 2012: First Amendment Challenges in the Digital Age*, STAN. TECH. L. REV., http://stlr.stanford.edu/symposia/2012-first-amendment-internet/ (last visited Apr. 30 2012).

[3] *Cf.* Shmoop Editorial Team, *Implied Privacy Rights in the Constitution*, SHMOOP U., INC. (Nov. 11, 2008), http://www.shmoop.com/right-to-privacy/implied-privacy-rights-constitution.html (last visited Apr. 30 2012).("[P]rivacy is one of those fundamental liberties guaranteed to us under the Fourteenth Amendment.").

[4] Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employment Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979 (2011).

protect you directly only against governments and state actors, but not typically against companies or individual social media users.[5] Where courts refer to constitutional or other privacy rights, they have to balance them against other civil rights. In the social media context, privacy interests are often pitched directly against rights to free speech and information. Communication freedoms generally trump privacy rights because the rights to free speech and information have been explicitly acknowledged in constitutions and human rights treaties around the world for centuries, and they have been recognized to afford particularly robust protections for media companies.[6]

¶3 Another reason why privacy expectations directed at social media companies tend to be misguided is that in the social media context, it is rarely the social media company that invades your privacy. What haunts people is typically user-generated content, i.e., information that people themselves, their friends, and other social media users upload. If other social media users disseminate offensive information, you may have claims against them under tort laws against libel and invasion of privacy. But, social media platform providers are not directly responsible for user generated privacy invasions. They can claim broad exemptions from contributory liability under existing laws that were intended to protect Internet service providers.[7]

¶4 You can also not expect much in terms of privacy entitlements under European-style data protection laws. Personal data about you that you and other users share on social media platforms for purely personal purposes are exempt from restrictions in data protection laws.[8] European data protection laws are intended to protect individual citizens from the dangers of data processing by governments and commercial businesses but not to curtail individual communications and information gathering. European data protection laws do not protect you from yourself or your friends.

¶5 If and when you use social media platforms, you are entitled to accurate disclosures regarding data processing practices of the platform operators. Under data protection, privacy, and competition laws, social media companies have to notify users or seek consent regarding data mining, behavioral advertising, and data sharing.[9] In this respect, however, your rights are not different from your rights against any other Internet company. For practical reasons, privacy disclosure requirements are less restrictive on social media platform operators than they are on operators of freely accessible web portals and information sites, because social companies require registrations and log-ins. When users register and log in, social media companies can easily provide privacy notices and obtain user consent. Most users click to accept privacy notices and consent declarations without reading or understanding them. Notice and consent requirements have not resulted in meaningful privacy protections—vis-à-vis social media platforms or any other companies.[10] And, most importantly, such

---

[5] As a rare exception, the California Constitution explicitly protects privacy and applies also to private actors, not only state actors. *See* CAL. CONST. art. 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy").

[6] LOTHAR DETERMANN, FREEDOM OF COMMUNICATIONS ON THE INTERNET 1 ET. SEQU. (1999).

[7] LOTHAR DETERMANN STEVE HOLMES, LARS BRAUER & SIU HA TANG, USER GENERATED CONTENT SERVICES: THE UK AND US PERSPECTIVES, PLC CROSS-BORDER SERVICE AND PLC IP&IT SERVICE (2007); Lothar Determann & Saralyn Ang-Olson, *Recognition and Enforcement of Foreign Injunctions in the United States* - Yahoo!, Inc. v. La Ligue contre Le Racisme et L'Antisemitisme, COMPUTER L. REV. INT'L., 2002, at 12, 56; Lothar Determann, *Case Update - German CompuServe Director Acquitted*, 23 HASTINGS INT'L & COMP. L. REV. 109 (1999); Lothar Determann, *The New German Internet Law*, 22 HASTINGS INT'L & COMP. L. REV. 113 (1998). *But see Google Bosses Convicted in Italy*, BBC NEWS (Feb. 24, 2010), http://http://news.bbc.co.uk/2/hi/8533695.stm (reporting an Italian court's conviction of three Google executives for violating Italian privacy laws by allowing a video of an autistic teenager being bullied to be posted onto YouTube).

[8] Commission Directive 95/46/EC, art. 3.2, 1995 O.J. (L 281) 31 (providing that "This Directive shall not apply to the processing of personal data . . . by a natural person in the course of a purely personal or household activity.").

[9] Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good, Dietrich J. Wambach & Mika D. Ayenson, *Can Advertisers Learn That "No Means No"?*, Privacy & Sec. L. Rep. (BNA) 1398 (Sept. 26, 2011).

[10] *See, e.g.*, The Center for Democracy and Technology (CDT), *Rethinking the Role of Consent in Protecting Health Information Privacy*, Jan. 2009 at 8 *available at* http://www.cdt.org/healthprivacy/20090126Consent.pdf (last visited April 13, 2012); CDT AND THE MARKLE FOUNDATION, BEYOND CONSUMER CONSENT: WHY WE

notice and consent requirements apply only to the data processing practices of social media companies with respect data they collect from their users (through registration forms and cookies).[11] These requirements do not apply with respect to the user-generated data that is posted on social media platforms. Yet, it is the data that users post about themselves and others that tends to affect privacy interests most significantly. You have no privacy rights against social media companies in that regard.

MYTH 2: YOU OWN PERSONAL DATA ABOUT YOU

¶6 Talk about informational self-determination[12] and proposals for property law regimes to protect privacy[13] sometimes gives people the idea that they own personal data about themselves.[14] Fact is that no one owns facts. Factual information is largely excluded from intellectual property law protection: copyright law protects only creative expression, not factual information.[15] Trade secret law protects information that companies keep secret if such information derives an economic value from being secret.[16] Personal information about you that you or others post on social media platforms, however, is not secret and thus not subject to trade secret law protection. When social media companies aggregate information about usage and user preferences, the social media companies can claim trade secret ownership rights in such aggregate information, but they own such trade secrets and you do not. Also, databases with content and personal information can be protected under European database laws[17] and U.S. state laws on appropriation,[18] but again, as property of the social media companies and not as your personal property. So, if anyone owns personal data about you, it is the social media companies, not you.[19]

NEED A COMPREHENSIVE APPROACH TO PRIVACY IN A NETWORKED WORLD, (2008), *available at* http://www.cdt.org/healthprivacy/20080221consentbrief.pdf (last visited April 13, 2012); Nancy J. King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices*, 60 FED. COMM. L.J. 229 (2008); *see also* Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2074-75 (2004); Joseph Goldstein, *For Harold Lasswell: Some Reflections on Human Dignity, Entrapment, Informed Consent, and the Plea Bargain*, 84 YALE L.J. 683, 691 (1975); Peter H. Schuck, *Rethinking Informed Consent*, 103 YALE L.J. 899, 942–48 (1994).

[11] Lothar Determann, *How to Ask for a Cookie: Information Technology, Data Privacy and Property Law Considerations*, 15 Electronic Com. & L.Rep. (BNA) 8 (Feb. 24, 2010).

[12] See frequent references to "your own data" in press releases by the European Commission in the context of its new regulatory proposals, *e.g.*, EUROPEAN COMMISSION, HOW WILL THE DATA PROTECTION REFORM AFFECT SOCIAL NETWORKS? (2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf (last visited March 25, 2012).

[13] *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004); Lawrence Lessig, *Privacy as Property*, 69 SOC. RESEARCH 247 (Spring 2002).

[14] *Cf.* Paula Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1130 (2000) (discussing, then refuting, reasons why individuals might naturally assume they own data about themselves).

[15] *See, e.g.*, 17 U.S.C. § 102(b) ("In no case does copyright protection . . . extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery . . . ."); Feist Publications, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 347-48 (1991) (holding that "all facts – scientific, historical, biographical, and news of the day" are part of the public domain and are not copyrightable because they do not owe their origin to an act of authorship as required by Article I, § 8, cl. 8 of the U.S. Constitution for protection) (citations omitted).

[16] *See, e.g.*, Cal. Civ. Code § 3426.11.

[17] Commission Directive 96/9/EC of March 11, 1996 on the legal protection of databases, 1996 O.J. (L 77) (offering copyright-like protection to creators of valuable data bases).

[18] *See, e.g.*, Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 852-54 (2d Cir. 1997) (discussing the merits of a "hot news" misappropriation claim in the context of the unauthorized electronic delivery of near-real-time professional basketball statistics) (citations omitted); United States Golf Ass'n v. Arroyo Software Corp., 69 Cal. App. 4th 607, 611-12, 618 (1999) (discussing California's common law misappropriation as applicable to the unauthorized use of golf handicap formulas that were developed through intensive data collection and analysis); Bd. of Trade City of Chicago v. Dow Jones and Co., 439 N.E.2d 526, 537 (Ill. App. Ct. 1982) (applying Illinois' common law misappropriation to the unauthorized use of the Dow Jones Index and Averages as a trading vehicle); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 (1995); Jane C. Ginsburg, *Copyright, Common Law, and Sui Generis Protection of Data-Bases in the United States and Abroad*, 66 U. CIN. L. REV. 151, 157 et seq. (1997).

[19] But social media companies can, and often do, voluntarily and expressly disclaim property rights to user-

MYTH 3: EUROPEAN PRIVACY LAWS ARE BETTER, AND THE UNITED STATES HAS TO CATCH UP

¶7 Claims have been made for a long time that the European data protection law regime is more effective than the U.S. approach, often in support for federal legislation in the United States.[20]

¶8 Fact is that the U.S. approach to privacy legislation is *different* from the European approach: Congress reviewed and consciously rejected a proposal for European-style, omnibus privacy legislation in 1974.[21] Since then the U.S. has been addressing data processing activities only with respect to specific, compelling threats, via general consumer protection laws and narrowly crafted statutes.[22] U.S. laws have been enforced effectively in practice[23] and also have been continuously supplemented and updated to address specific threats; for example, data security breach notification laws were passed in California in 2002.[24] European legislatures, on the other hand, have tried since 1970 to regulate the processing of personal data through broad, omnibus legislation based on a general prohibition of automated data processing with limited exceptions, requiring companies to obtain prior government approvals for many data-related activities. European data protection laws have not historically differentiated much with respect to particular threats, industries, or types of data.[25] They have remained relatively static over the years. Enforcement by data protection authorities has been lax throughout much of the European data protection laws' history and private enforcement has been nearly non-existent.[26] Thus, differences between U.S. data privacy and European data protection laws are indeed significant.

¶9 It is hardly a proven fact, however, that European data protection laws protect individual privacy better than the U.S.[27] Due to the historic lack of enforcement of data protection laws in Europe, there is still a wide gap between assertions by European data protection authorities and legal commentaries as to what is allowed and forbidden and what companies and government authorities are actually doing and getting away with. In many ways, European data protection laws are

---

generated content in their terms of use. See, for example, the Facebook Statement of Rights and Responsibilities: "Sharing Your Content and Information. You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. (…), http://www.facebook.com/legal/terms; Yelp Terms of Service: "Ownership. As between you and Yelp, you own Your Content," http://www.yelp.com/static?p=tos&country=US.

[20] *See, e.g.*, *Hearing on the European Union Data Directive and Privacy, Before the H. Comm. on Int'l Rel.,* 105th Cong. (1998) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center), *available at* http://epic.org/privacy/intl/rotenberg-eu-testimony-598.html.

[21] Paul Schwartz, *Preemption and Privacy*, 118 YALE L. J. 902, 910 (2009).

[22] *See* Schwartz, *supra* note 21 at 118; *see also* DANIEL J. SOLOVE AND PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS (2011).

[23] *See* Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 O.J. (L 215) 7, 26-38 (giving a comprehensive assessment of U.S. enforcement).

[24] Cal. Civ. Code §§ 1798.29, 1798.82.

[25] Schwartz, *supra* note 21 at 910.

[26] *See* Ruth Hill Bro, *Life in the Fast Lane: Government Enforcement and the Risks of Privacy Noncompliance*, 6 Privacy & Sec. L. Rep. (BNA) 32 (Aug. 6, 2007) (containing reports on the first significant enforcement actions in Europe, which did not materialize until the mid-2000s, over 30 years after the first data protection laws were enacted in Europe).

[27] *Compare* Schwartz, *supra* note 21 at 946 (2009) (arguing that the United States should not adopt a federal omnibus information privacy law with strong preemption provisions such as the European Data Privacy Directive because such a law would limit experimentation in federal and state sectoral laws, and would be difficult to amend, thereby becoming outdated as technological changes undermine the law's regulatory assumptions) *with* Marsha Cope Huie, Stephen F. Laribee & Stephen D. Hogan, *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391 (2002) (arguing that the United States should revise its privacy laws so as to embrace the European 1995 Data Privacy Directive) *and* Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357 (2005) (suggesting that the United States pattern its privacy laws after Canada's, which are argued to be a middle ground between the United States' piecemeal approach and the European Union's omnibus regime).

overbroad, under-enforced, outdated and awaiting reality checks in courts. Take data security breaches, for example: the broad, omnibus information requirements under existing European data protection laws have arguably always required companies to inform data subjects of security breaches,[28] however, in practice European companies have rarely disclosed breaches.[29] Now, ten years after California passed the first law specifically requiring data security breach notifications, the European Union is working on similar legislation to address the serious threats to data security that have become acute in the last two decades.[30] In general, the European Union considers its own privacy law regime so deficient and outdated that it has recently proposed a complete overhaul, specifically referencing a need to update the rules on personal data in social media.[31] Thus, it seems a myth that the European Union is somehow ahead of the U.S. in terms of social media privacy protections.

¶10 With respect to personal data on social media platforms, the current European data protection regime offers hardly any protection at all given that European data protection laws exempt data processing by individuals for personal and private household purposes.[32] The only aspect of social media privacy protection that is covered by existing omnibus European data protection laws is data collection by social media companies for their own purposes, primarily through registration processes and cookies. With respect to data collection through cookies and other tracking technologies, the general European data protection laws from the early 1970s would already seem to require Internet companies to obtain prior, informed, voluntary, specific, express, and written consent, given that no other exception allowing this practice was provided for in statutes.[33] In this respect, the European omnibus legislation approach could have offered superior protection for individual data privacy, because the general prohibition of automated data processing should have captured cookie placement at the outset, without any need for special or updated legislation, whereas the United States' approach would have left consumers unprotected until threats evolved and the legislature or the courts reacted. But, this would have been true only if anyone had taken the broad European omnibus laws seriously. This is not how things played out in practice, though. Companies placed cookies in the United States and Europe without asking for consent. European data protection authorities did not enforce their laws and in 2002, the European Union passed special legislation sanctioning the practice by allowing companies to place cookies unless users opted out.[34] In 2009, the European union made an effort to restore what seems to have been the law all along since 1970 and required companies to obtain prior opt-in consent before they placed cookies for marketing

---

[28] *See* Council Directive 95/46/EC, art. 10, 1995 O.J. (L 281) (providing that companies ". . . must provide a data subject . . . with at least the following information . . . : (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject."). Because data subjects have to be informed about data "recipients or categories of recipients," it would seem to follow that data controllers would have to inform data subjects if their data is received by unauthorized persons. But, judging by the historic absence of breach notifications in Europe, the Europeans seem to understand this very broad wording to cover only "recipients in the normal course of business," with the effect that European data subjects are getting plenty of information on relatively mundane and legitimate data sharing, but not the very crucial information on data security breaches that they would need to protect themselves.

[29] In the few situations where companies issued notices, authorities responded with severe fines. *See, e.g.*, Ali Qassim, *E.U. Data Protection: U.K.'s ICO Issues First Privacy Fines Under New Authority to Issue Penalties*, 9 Privacy & Sec. L. Rep. (BNA) 1669 (Dec. 6, 2010); Donald Aplin, *U.K. Finance Services Regulator Fines Insurer $3.49 Million for Data Breach in Outsourcing*, 9 Privacy & Sec. L. Rep. (BNA) 1253 (Sept. 6, 2010).

[30] *See* Council Directive 2009/136/EC, 2009 O.J. (L 337) 11 (implemented on May 25, 2011).

[31] *See Commission proposes a comprehensive reform of the data protection rules*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (last visited March 25, 2012).

[32] Council Directive, *supra* note 8.

[33] *See* Council Directive 95/46/EC, art. 7, 1995 O. J. (L 281) 31, 44.

[34] Council Directive 2002/58/EC, 2002 O.J. (L 201) 37.

purposes.[35] Many of the European Economic Area member states are dragging their feet on the implementation, however, and it remains to be seen whether the "remake" will be taken more seriously than the "original."

¶11 In the meantime, U.S. social media companies are offering their services very successfully and without significant modifications in Europe. Europeans use such services much like U.S. users. Some European government agencies are taking steps to enforce local laws,[36] but so are U.S. authorities[37] and class action attorneys.[38] Thus, all in all, European data protection laws do not appear to be ahead of U.S. laws or appear to protect privacy interests with respect to social media better than do U.S. privacy laws.

¶12 European data protection laws however, may have made a difference in practice in one regard: most meaningful innovation in the information and social media age has been coming from U.S. companies, not Europeans.[39] This may be due to the fact that the hostile regulatory environment with broad prohibitions on data processing technologies has been deterring early-stage entrepreneurs and investors. But this also does not make the European data protection laws better or support claims that the United States should catch up.

MYTH 4: SOCIAL MEDIA COMPANIES THREATEN YOUR PRIVACY

¶13 Some people attribute whatever privacy intrusion occurs in a social media context to the companies that operate the networks.[40] Fact is that some social media companies have had to settle privacy related lawsuits and charges.[41] Missteps are part of growing pains of any new industry,

---

[35] Council Directive 2009/136/EC, 2009 O.J. (L 337) 11.

[36] Brett King, *Spain's DPA Vows Move to Sanctions For Web Company Privacy Violators*, 9 Privacy & Sec. L. Rep. (BNA) 1663 (Dec. 6, 2010); Jabeen Bhatti, *German State Data Protection Authorities Demand Compliance From Social Networks*, 11 Privacy & Sec. L. Rep. (BNA) 472 (Mar. 12, 2012); Julian Hale, *Ireland DPA Issues Facebook Privacy Audit, Social Media Giant Agrees to Make Changes*, 11 Privacy & Sec. L. Rep. (BNA) 23 (Jan. 2, 2012); Decision on complaint by a German consumer protection watchdog against Facebook, LG Berlin, No. 16 O 551/10, 3/6/12, *available at* http://op.bna.com/pl.nsf/id/dapn-8sck2t/$File/facefind.pdf.

[37] *See*, *e.g.*, Complaint, Facebook, Inc., FTC File No. 092 3184 (Nov. 29, 2011); Complaint, Google, Inc., FTC File No. 102 3136 (Mar. 30, 2011); Complaint, Twitter, Inc., FTC File No. 092 3093 (June 24, 2010).

[38] *See*, *e.g.*, Low v. LinkedIn Corp., No. 11-CV-01468-LHK, 2011 WL 5509848 (N.D. Cal. 2011); *In re* Facebook Privacy Litigation, 791 F. Supp. 2d 705 (N.D. Cal. 2011) (motion to amend denied Feb. 21, 2012); Complaint, Opperman v. Path Inc., No. 1:12-CV-00219 (W.D. Tex. filed Mar. 12, 2012); Don Aplin, *Google Agrees to Pay $8.5 Million to Settle Buzz Application Consumer Class Actions*, 9 Privacy & Sec. L. Rep. (BNA) 1276 (Sept. 13, 2010).

[39] We shall see whether the European response to this phenomenon; even more and stricter regulation will indeed help Europe to catch up, as the European Commission claims in its latest proposals: "Why is this good for the digital economy? . . . [I]ndividual trust in online services is vital for stimulating economic growth in the EU. . . . [T]he new rules will put people in control of their personal data, and will foster trust both in social media and in online shopping and communication in general." EUROPEAN COMMISSION, HOW WILL THE DATA PROTECTION REFORM AFFECT SOCIAL NETWORKS? (2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf (last visited March 25, 2012).

[40] *See*, *e.g.*, Shea Bennett, *Are Twitter And Facebook A Serious Threat To Your Privacy?*, MEDIA BISTRO (Feb. 23, 2012 8:00 AM), http://www.mediabistro.com/alltwitter/social-media-privacy_b18922.

[41] *See, e.g.*, United States v. RockYou Inc., No. 12-cv-1487 (N.D. Cal. Mar. 28, 2012) (alleging that social gaming site, RockYou failed to implement reasonable safeguards to protect around 32 million users' unencrypted email addresses and passwords from one or more hacker breaches); Complaint, Google, Inc., FTC File No. 102 3136 (Mar. 30, 2011) (alleging that the now-defunct social networking service Google Buzz "did not adequately communicate that certain previously private information would be shared publicly by default," and that "the controls that would allow the user to change the defaults were confusing and difficult to find."); Complaint, Twitter, Inc., FTC File No. 092 3093 (June 24, 2010) (alleging that Twitter failed to provide reasonable and appropriate security to prevent unauthorized access to its users' private information). Complaint, Facebook, Inc., FTC File No. 092 3184 (Nov. 29, 2011) (alleging that the user data that Facebook designated as "publicly available" harmed users by threatening their health and safety, and exposed potentially controversial political views and other sensitive information and affiliations); *see also*, Nancy J. Moore, *Class Complaint Alleges Mobile App Makers Took Address Book Data Without Consent*, 11 Privacy & Sec. L. Rep. (BNA) 518 (Mar. 19, 2012) (reporting on a lawsuit that alleges that makers of mobile applications are harvesting private address book data from users' mobile devices without consent, according to a class complaint filed on March 12, 2012 in the United States District Court for the Western District of Texas, Opperman v. Path Inc., No. 1:12-CV-00219 (W.D. Tex. filed Mar. 12, 2012), naming as defendants Path Inc., Twitter Inc., Apple Inc.,

particularly one driven by new technologies and start-up companies operating in a rapidly developing legal environment. In the cases referenced earlier,[42] social media companies were primarily charged because of data security weaknesses and failure to provide sufficiently conspicuous notices when prompting consumers to consent to changes. Data security and consumer consent requirements have been in flux for years and companies in many industries have been struggling to keep up or catch up with the law.[43] It is no surprise that social media companies have also had difficulties clearing compliance hurdles as the bars are being raised.

¶14 There is no reason, however, to take such missteps as an indication that social media companies constitute a systematic threat to privacy. Social media companies are strongly incentivized to avoid harming users or prospective users. They are operated for profit and have to cater to user demands. Social media companies create technology platforms and offer features that users demand. Most privacy threats in the social media sphere have emanated from the manner in which people have used social media platforms.[44] Social media companies do not select or post any harmful information. Individual users add the personal data. If users cannot be social and share data on social media platforms, then they will disseminate information in person, over the phone, on Internet blogs, and elsewhere. The urge of individuals to be social and share information is what has the greatest effect on privacy. It is a myth that social media companies are to blame for this.

MYTH 5: ADVERTISERS THREATEN YOUR PRIVACY

¶15 Activists, academics and regulators are quite discontented with tracking, profiling and behavioral advertising.[45] The practices are also not particularly popular with users who understand them.[46] But can they really be perceived as a significant threat to privacy? Where is the harm?[47] All that advertisers want is to display more relevant advertisements to consumers. That in itself is hardly a bad thing. Relevant advertisements are better than irrelevant advertisements. Some consumers might prefer seeing no advertisements at all, or relevant advertisements without tracking. These options are not available in practice, though. Advertisers need tracking information to target ads, and social media companies need funding from advertisers in order to offer services free of charge to consumers. Without advertising dollars, Internet companies could never have created all the services that we have come to enjoy and depend on in our daily lives, including web search, maps and social media. Governments could not have created them with taxpayer money and paid services are much less quickly adopted and usually only on the heels of charge-free services.[48] Most consumers are more or less aware of the trade-off and the fact that they pay for services with their data and willingness to

---

Facebook Inc., Beluga Inc., Yelp! Inc., Burbn Inc., Instagram Inc., Foursquare Labs Inc., Gowalla Inc., Foodspotting Inc., Hipster Inc., LinkedIn Corp., Rovio Mobile Oy, ZeptoLab UK Ltd., Chillingo Ltd., Electronic Arts Inc., and Kik Interactive Inc.).

[42] *Id.*

[43] *See*, *e.g.*, Lothar Determann and Jesse Hwang, *Data Security Requirements Evolve: From Reasonableness to Specifics*, 26 COMPUTER & INTERNET L., no. 9, 2009, at 6; Lothar Determann, *Notice, Assent Rules for Contract Changes after Douglas vs. .U.S District Court*, 12 Electronic Com. & L. Rep. (BNA) 32 (Mar. 19, 2007).

[44] *See*, *e.g.*, Devlin Barrett, *Democrats Push Weiner To Go*, WALL ST. J., June 9, 2011, http://online.wsj.com/article/SB10001424052702304392704576374014222200024.html; Lothar Determann, *Social Media @ Work—A Checklist for Global Businesses*, 11 Privacy & Sec. L. Rep. (BNA) 487 (Mar. 19, 2012).

[45] Hoofnagle, *et al.*, *supra* note 9; Geoffrey A. Fowler, *Tech Giants Agree To Deal On Privacy Policies For Apps*, WALL ST. J., Feb. 23, 2012, at B4 (quoting California Attorney General Kamal D. Harris on social media apps: "We have populations without knowledge of [mobile technology's] potential uses who are potentially vulnerable . . . We seek to give them tools to protect themselves.").

[46] Lymari Morales, *US Internet Users Ready to Limit Online Tracking for Ads*, GALLUP (Dec. 21, 2010), *available at* http://www.gallup.com/poll/145337/internet-users-ready-limit-onlinetracking-ads.aspx (reporting that in a Gallup Poll, 61 percent of American adults felt that online behavioral advertising was not justified because "the free access [to websites] is not worth the invasion of privacy involved.").

[47] *See generally* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L. J. 1131 (2011).

[48] For example, it has taken years of free public television, followed by advertising-funded private television until ad-free pay television could establish itself.

endure ads. They are also quite willing to allow tracking offline. For example, shoppers routinely let retailers build extensive profiles on their consumption habits in return for a small discount.[49] Of course, it is possible that user profiles built by advertisers can be abused by others. For example, health insurance companies and employers could use information in user profiles to discriminate against sick people if they gain access;[50] but, such threats to privacy emanate primarily from the practices of health insurance companies and employers. Such concerns should be—and are[51]—addressed in insurance regulations and labor laws. Another group of commonly cited examples relates to fears regarding abuse of user profiles by criminals and governments.[52] Such fears also do not support attempts to cast advertisers as the primary threat to privacy, because criminals and governments play the lead role in these horror stories and point to solutions in the form of stricter laws on data security and government access. But this consideration presents a good transition to the next myth.

MYTH 6: LAW ENFORCEMENT SHOULD BE KEPT OUT OF SOCIAL MEDIA IN THE INTEREST OF BETTER PRIVACY PROTECTION

¶16 Reports of aggressive online investigative methods by governments around the world are good for catchy headlines.[53] It is a fact that law enforcement authorities investigate suspects and that investigations intrude into people's privacy. Social media companies, telecommunication companies and Internet Service Providers themselves complain that governments are overreaching in many cases.[54] It is also a well-known fact, however, that law enforcement authorities often act to protect children and consumer data privacy and security. Governments pursue spammers, cybercriminals and fraudsters who hack into accounts, steal identities and invade privacy.[55] Law enforcement protects one's privacy. In *United States v. Councilman*, for example, the FBI pursued the operator of an online community with a shared interest in rare books for interception of emails sent via his platform. The FBI charged Councilman with violations of U.S, privacy laws and conceded in the process that email interception constitutes a violation of federal wiretap laws,[56] a factor that is suited to restrict the FBI's own ability to conduct investigations online. Thus, it is misleading to portray law enforcement authorities as a threat to privacy. More accurately stated, law enforcement is necessary to protect data privacy and security on social media.

---

[49] Martin Bosworth, *Loyalty Cards: Reward or Threat?*, CONSUMER AFFAIRS (July 11, 2005), http://www.consumeraffairs.com/news04/2005/loyalty_cards.html.

[50] *Online Tracking and Behavioral Profiling*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/consumer/online_tracking_and_behavioral.html (last visited Feb. 23, 2012).

[51] *See, e.g.*, *California Bill Would Ban Demands for Worker, Job Applicant, Student Social Media Passwords*, 11 Privacy & Sec. L. Rep. (BNA) 600 (Apr. 4, 2012); Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881.

[52] *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

[53] *See* Dominic Rush, *FBI To Step Up Monitoring Of Social Media Sites Amid Privacy Concerns*, THE GUARDIAN, Jan. 26, 2012, http://www.guardian.co.uk/world/2012/jan/26/fbi-social-media-monitoring-privacy/print (quoting Lillie Coney, associate director of EPIC: "They [the FBI] are going to launch investigations and start looking at all sorts of people [on social networks] that they have no right to be investigating. There is no accountability, transparency or oversight.").

[54] *See* DIGITAL DUE PROCESS, http://digitaldueprocess.org (last visited March 25, 2012).

[55] *See* Press Release, U. S. Attorney's Office, N. Dist. of Ga., Three Romanian Citizens Sentenced for Internet Scam (Mar. 13, 2012), *available at* http://www.justice.gov/usao/gan/press/2012/03-13-12.html (reporting that three Romanian citizens were sentenced to U.S. federal prison for an Internet fraud scheme to collect money from fake advertisements for cars and merchandise); Stacy Cowley, *FBI Director: Cybercrime Will Eclipse Terrorism*, CNN.COM (Mar. 2, 2012), http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/ index.htm (noting the FBI's 56 cybersecurity squads and 1,000 agents and analysts who work the "Web beat"); Bruce Vielmetti, *Milwaukee FBI Agent Trips Up Russian 'King of Spam'*, JOURNAL SENTINEL, Dec. 1, 2010, http://www.jsonline.com/news/crime/111169714.html (discussing the United States' indictment and arrest of a man responsible for one-third of the global spam stream).

[56] United States v. Councilman, 418 F.3d 67, 70 (1st Cir. 2005).

MYTH 7: TECHNOLOGIES THREATEN YOUR PRIVACY

¶17 If social media companies, advertisers, and law enforcement are not to blame as the primary threat to privacy, is it perhaps the new technologies themselves?[57] No. Technologies do not invade privacy, people with technologies invade privacy.[58] You and your friends are a threat to your privacy.

MYTH 8: YOU HAVE A RIGHT TO BE FORGOTTEN

¶18 While technology innovators in the United States are working hard to be remembered, European politicians are obsessed with a right to be forgotten.[59] This makes for quite a symbolic illustration of the transatlantic divide between the new and old world with respect to innovation in the information age. The fact that the "right to be forgotten" is presented in the form of new legislation demonstrates that it is not currently the law, not even in Europe.[60] Fact is that you currently have rights to remain silent, keep information about you confidential, obtain injunctions against defamation, and demand correction of inaccurate information. But, just as you do not own information about yourself, you do not have a general right to demand that others delete all information about you. Other people have a right to inform themselves about the world, including about you. The right to free speech and information is protected against government interference in most constitutions around the world.[61]

¶19 A *desire* to be forgotten sounds a bit pathetic, but a *right* to be forgotten, to control other people's memory, sounds outright scary--straight from George Orwell's vision of 1984 actually, where the

---

[57] *See* Riva Richmond, *12 Ways Technology Threatens Your Privacy (and How to Protect Yourself)*, SWITCHED (May 14, 2009), http://www.switched.com/2009/05/14/12-ways-technology-threatens-your-privacy-and-how-to-protect-yo/ (describing the privacy threats of phishing, malware and spyware, social-networking sites, photo and video sharing, histories of web use, targeted advertising, installing cookies, cloud computing, electronic medical data, public wi-fi, loyalty cards from retail stores, workplace surveillance, and cellular phone tracking).

[58] This is true for various tools and technologies, see *Quotes About Guns and Other Things That 'Don't Kill People'…*, QUOTE/COUNTERQUOTE, http://www.quotecounterquote.com/2011/03/guns-dont-kill-people-people-kill.html (last visited Mar. 4, 2012).

[59] *See EU Proposes 'Right To Be Forgotten' By Internet Firms*, BBC NEWS (Jan. 23, 2012), http://www.bbc.co.uk/news/technology-16677370 (discussing the EU's proposed regulation requiring firms to delete data about users upon request if there are no "legitimate grounds" for the data to be kept); Bruno Waterfield, *'Right To Be Forgotten' Proposed By European Commission*, THE TELEGRAPH, Nov. 5, 2010, http://www.telegraph.co.uk/technology/news/8111866/Right-to-be-forgotten-proposed-by-European-Commission.html (quoting Viviane Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship: "Internet users must have effective control of what they put online and be able to correct, withdraw or delete it at will . . . . [T]he right to be forgotten is essential in today's digital word."); Joseph Turow *et al.*, *Americans Reject Tailored Advertising and Three Activities That Enable It* (Sept. 29, 2009) (working paper), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 (reporting that in a random survey of 1,000 American adults, 92% believed that there should be a law requiring "websites and advertising companies to delete all stored information about an individual, if requested to do so"). European politicians have claimed a right to have certain information about them forgotten before. For example, Germany's former chancellor, Konrad Adenauer is quoted with the following response to an accusation of flip-flopping: "Was geht mich mein Geschwätz von gestern an [What do I care about my ramblings of yesterday]." ZITATE-ONLINE, *Was Interessiert Mich Mein Geschwaetz von Gestern An*, http://www.zitate-online.de/sprueche/politiker/15426/was-interessiert-mich-mein-geschwaetz-von-gestern.html (last visited May 5, 2012).

[60] *See* Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), at 51, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. The EU Commission refers to a 'strengthening' of a supposedly existing right, but current data protection laws in Europe only provide for very limited correction and deletion rights regarding data that governments and businesses collect.

[61] *E.g.*, CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA, 1996, Ch. 2, § 16(1)(b) (granting freedom of expression and freedom to receive or impart information or ideas); BUNDESVERFASSUNG [BV] [CONSTITUTION] Apr. 18, 1999, SR 101, art. 16 (Switzerland) (granting the right to free expression and the right to receive, gather, and disseminate information from generally accessible sources); SALIGANG BATAS NG PILIPINAS [CONSTITUTION] 1987, art. III, §§ 4, 7 (Philippines) (granting the right to freedom of speech and expression, and the right to information on matters of public concern). *See generally* LOTHAR DETERMANN, KOMMUNIKATIONSFREIHEIT IM INTERNET : FREIHEITSRECHTE UND GESETZLICHE BESCHRÄNKUNGEN [FREEDOM OF COMMUNICATIONS ON THE INTERNET] (1999).

government was also obsessed with constantly re-writing history and controlling citizen's memories.[62] The European Commission apparently wants to entitle everyone to demand erasure of information, including text and pictures created by other friends, family and other users in other users' accounts.[63] This will cause significant intrusions into other people's rights.

¶20 A right to be forgotten would also create a colossal administrative burden.[64] Someone would have to pay for the detection and deletion of data that can end up in myriad accounts and places in social networks. Social media platform operators could either charge the data subject who exercises the right to be forgotten or all users. Commercially successful, well-established social media platform providers could also cover the compliance costs themselves out of profits generated through sales of advertising, but start-up companies with charge-free business models would be unduly burdened if they cannot pass on costs. This could further hamper innovation in Europe.

¶21 During the 2012 Symposium of the Stanford Technology Law Journal on "First Amendment Challenges in the Digital Age,"[65] Professor Franz Werro argued for a right to be forgotten in reference to an incident that recently occurred in Switzerland: a bank robber had served a long prison sentence, then started a new career and became a successful businessman. Many years later, a journalist tracked him down and reported on his past, putting his new existence in jeopardy. Professor Werro argued that the ex-convict-turned-successful-businessman has a right to have his past forgotten. I argued against such a right by pointing to the right of the public to remain informed, and the value of this particular story for public opinion and society: the fact that the convict was able to successfully re-integrate himself into society should be made known to the public to dispel prejudice and help reform the justice system. If these facts are made sufficiently known, then in the future, people do not have to beg that their pasts be forgotten.

¶22 Whether it is necessary to refer to the individual convict's name in the press is certainly debatable. European news media does not usually refer to individuals' names except regarding public figures, whereas it is rather common in the United States to name everyone, whether famous or not. Whether the Swiss press should have named the bank robber's real name in the original reports about his conviction or in the subsequent reports about his re-integration into society is a separate question from the question of whether he should have a right to be forgotten. Maybe he should not have been named in either the robbery or the re-integration reports. If Swiss law allows naming the bank robber right after he committed the deed, however, the same law should probably not be opposed to naming him again in positive news on his re-integration into society. But either way, his story should not be forgotten.

¶23 It is also not settled yet whether today's children will want or need a right to be forgotten as they grow up. Google's former CEO Eric Schmidt has suggested that today's children may have to change their names when they turn thirty, to have their pasts forgotten and disassociate themselves from all the sensitive, potentially embarrassing information that they and their friends publish about them on social media sites.[66] But perhaps, instead, social media will foster tolerance and soon there will be so

---

[62] *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

[63] EU Commission Factsheet, How will the data protection reform affect social networks?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf.

[64] To support the creation of a 'right to be forgotten,' the EU Commission refers to the following story: "An Austrian law student requested all the information that a social networking site kept about him on his profile. The social network sent him 1,224 pages of information. This included photos, messages and postings on his page dating back several years…" EU Commission Factsheet, How will the data protection reform affect social networks?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf. The EU Commission does not explain how it anticipates that social media platform providers are supposed to track down all this information in all other users' accounts, cache files, back-up tapes, email accounts, etc., and then delete only the personal information of the person who wants to be forgotten, without unnecessarily causing damage to letters, information, photos, etc., collected legitimately by other users, and how to allocate the resulting costs.

[65] *Symposium 2012: First Amendment Challenges in the Digital Age*, STAN. TEC. L. REV., http://stlr.stanford.edu/symposia/2012-first-amendment-internet/ (last visited Apr. 30 2012).

[66] Holman W. Jenkins Jr., *Google and the Search for the Future*, WALL ST. J., Aug. 14, 2010, http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html.

much embarrassing information about everyone online that society will learn to accept the fact that youngsters may be wild and take extreme views. Maybe once our children turn thirty, society will have become less hypocritical and accept that young people have a right to change their views. Then, hopefully, no one has to wish to be forgotten, hide their past, and change their name.

MYTH 9: YOU HAVE A RIGHT TO REMAIN ANONYMOUS ON THE INTERNET

¶24 Some bloggers and social media users seem to believe that they are entitled to lie about their names in registration processes and hide behind fake identities.[67] Internet sites that want to attract and protect uncensored speech, radical opinions, and political dissidents will typically allow users to choose fantasy names. But, just as a homeowner or a hotel owner has the right to verify the identity of a guest who wants to set foot on her property, operators of social media sites have a legitimate interest and right[68] to require truthful identity information and that people use their real names on the site. Social media platforms that want to minimize disputes between users or with third parties may prefer to require everyone to use their real name, because "[p]eople behave a lot better when they have their real names down."[69] If in spite of such requirements users provide fake names, then they breach contract terms, trespass on servers, and potentially violate computer interference laws, such as the U.S. Computer Fraud and Abuse Act.[70]

MYTH 10: SOCIAL NETWORKS ARE NOT—BUT SHOULD BE—SUBJECT TO LAWS

¶25 Whenever new technologies establish themselves, people wonder whether no laws apply yet. Some wish to preserve the presumed legal no-man's-land status while others scream for specific legislation.[71] When the Internet first became popular, some were quick to declare the independence of cyberspace[72] while others demanded new laws.[73] Similar claims surfaced when virtual worlds arrived on the radar of public opinion.[74] New technologies often make politicians wonder whether

---

[67] *See* Aaron Morris, *Law Student Blogger Fights to Remain Anonymous*, INTERNET DEFAMATION BLOG (Oct. 15, 2011), http://internetdefamationblog.com/law-student-blogger-fights-to-remain-anonymous/ ("[T]here is a constitutional right to remain anonymous on the Internet. The concept harkens back to the days of 'pamphleteers'—those who could distribute anonymous pamphlets, usually criticizing the government. The authors of these pamphlets needed to remain anonymous lest they be harassed by the government officials they were criticizing. Any requirement that pamphleteers sign their work was deemed to be an unconstitutional violation of the First Amendment. Today's pamphleteers use the Internet and sometimes have a compelling need to remain anonymous.").

[68] Exceptions apply. For example, under German law, providers of online media services have to allow users to use and pay for services anonymously or under a pseudonym if and to the extent technologically possible and reasonably acceptable to the service providers' interests. Telemediengesetz [TMG] [Telemedia Act], Feb. 26, 2007, BUNDESGESETZBLATT, Teil I [BGBL. I] at 179, §16(6) (Ger.), *available at* http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf (last visited April 13, 2012).

[69] Bianca Bosker, *Facebook's Randi Zuckerberg: Anonymity Online 'Has To Go Away'*, THE HUFFINGTON POST (July 27, 2011, 1:23 PM), http://www.huffingtonpost.com/2011/07/27/randi-zuckerberg-anonymity-online_n_910892.html.

[70] *See*, *e.g.*, United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009) (a woman impersonated a teenage boy on MySpace.com and used the account to bully a teenage girl, causing the girl to kill herself); Ticketmaster L.L.C. v. RMG Techs., Inc., 507 F. Supp. 2d 1096, 1116-17 (C.D. Cal. 2007) (enjoining the RMG, *inter alia*, from marketing and selling automated devices that circumvented Ticketmaster's technological copy protection systems to purchase large quantities of tickets).

[71] *See*, *e.g.*, Robert E. Lemons, *Protecting Our Digital Walls: Regulating the Privacy Policy Changes Made by Social Networking Websites*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 603, 614-18 (2011) (discussing the need for a regulatory framework for social networking sites and proposing such a framework).

[72] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, EFF, https://projects.eff.org/~barlow/Declaration-Final.html (last visited Feb. 18, 2012).

[73] *Cf.* Lothar Determann, *The New German Internet Law*, 22 HASTINGS INT'L & COMP. L. REV. 113, 116 (1998); Ari Staiman, *Shielding Internet Users from Undesirable Content: The Advantages of a Pics Based Rating System*, 20 FORDHAM INT'L L.J. 866, 866 (1997) (citing a European Commission Green Paper which said "We know that national regulation … is not enough, that European regulation is not enough … We may need to have a world regulation of these matters."

[74] Lawrence J. Speer, *French Internet Rights Forum Proposes New Legal Rules for Online Games*, 12 Electronic

fundamental regulatory or statutory gaps exist. Upon closer review, however, this is relatively rarely the case.[75] Existing rules can be and are, in fact, continuously applied to new technological, economic, and social developments, supplemented and adapted from time to time.[76]

MYTH 11: SOCIAL MEDIA USAGE ISN'T, CAN'T BE, OR SHOULDN'T BE REGULATED BY EMPLOYERS

¶26 The U.S. National Labor Relations Board seems to believe that any criticism of an employer by employees on social media constitutes a protected concerted action.[77] The European Court of Human Rights also recently emphasized the rights of employees to criticize their employer.[78] Yet, for the most part, employers are regulating employee activities on social media platforms similar to how they regulate other employee conduct[79] and it remains to be seen whether courts will apply special standards for labor cases relating to social media usage. Fact is that most employee handbooks and other work rules already address many of the concerns raised by social media. Therefore, employers do not have to come up with any fundamentally new rules for social media. Employers merely have to consider how to apply and adapt existing rules to new social media platforms, to benefit from the many opportunities that social media offer (*e.g.*, for collaboration and marketing), and also to mitigate against risks (*e.g.*, trade secret disclosures, losses of productivity, violations of anti-spam laws, harassment of co-workers, third party copyright infringements, illegal endorsements, etc.).[80] Also, employers have to carefully consider if and how to use information on social media platforms to vet job candidates[81] or investigate employee misconduct.[82] So, fact is that employees' social media usage is, can be and should be regulated by employers.

Com. & L. Rep. (BNA) 1189 (Dec. 5, 2007).

[75] Recall how, in 2004, the California senate was quick to pass a new law restricting the placement of ads into emails when a charge-free email service with targeted ads based on automated analysis technology was launched , only to withdraw the bill a few weeks later when realizing that existing California law was strict enough – and probably even stricter than the proposed new statute. *See* Evan Hansen, *California Senate Approves Anti-Gmail Bill*, CNET NEWS (May 27, 2004), http://news.cnet.com/California-Senate-approves-anti-Gmail-bill/2100-1028_3-5222062.html; *Calif. Bill to Bar E-Mail Scans Withdrawn; Paper Records Privacy Amendment Dies*, 3 Privacy & Sec. L. Rep. (BNA) 954 (Aug. 16, 2004); Seven years later, the pre-2004 laws were invoked in a class action lawsuit that appears absurdly outdated. *See* Thomas Claburn, *Google Sued Over Gmail Content Scanning*, INFO. WEEK (Nov. 19, 2010), http://www.informationweek.com/news/smb/hardware_software/228300269. Eric Goldman characterizes the complaint as an "are-you-kidding-me? lawsuit" on his blog. Eric Goldman, *"Trends in Internet Law" Talk Slides*, TECH. & MARKETING BLOG (Nov. 18, 2010), http://blog.ericgoldman.org/archives/2010/11/trends_in_inter.htm; Thomas Claburn, *Google Sued Over Gmail Content Scanning*, INFORMATION WEEK (Nov. 19, 2010), http://www.informationweek.com/news/228300269 (quoting Eric Goldman, "Frankly, after all the furor died down a half-decade ago, I had assumed everyone had moved on long ago.").

[76] *See also* Lothar Determann, *supra* note 60; LOTHAR DETERMANN, NEUE GEFAHRVERDÄCHTIGE TECHNOLOGIEN ALS RECHTSPROBLEM-BEISPIEL: MOBILFUNK-SENDEANLAGEN [NEW, POTENTIALLY DANGEROUS TECHNOLOGIES AS A LEGAL ISSUE - EXAMPLE: MOBILE PHONE STATIONS] (1996); *cf.* Tamara Russel, *Employment/Labor Law Meets Social Media: Advice for Employers*, 10 Privacy & Sec. L. Rep. (BNA) 1166 (Aug. 15, 2011); Paul H. Klickermann, *Virtuelle Welten ohne Rechtsansprüche?*, MULTIMEDIA UND RECHT, no. 12, 2007, at 766.

[77] *JT's Porch Saloon & Eatery Ltd.,* NLRB Div. of Advice, No. 13-CA-46689; *Martin House,* NLRB Div. of Advice, No. 34-CA-12950; *Wal-Mart,* NLRB Div. of Advice, No. 17-CA-25030; *see also NLRB Advice Division Finds No Protection For Some Employee Complaints on Facebook*, 10 Privacy & Sec. L. Rep. (BNA) 1117 (Aug. 8, 2011); *Party names withheld*, No. BS 150-1946/2009 (DK (Horsens) Ct., May 23, 2011), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-8lgs58; *Danish Firms May Rely on Social Media Posts to Fire Disloyal Workers, But Within Limits*, 10 Privacy & Sec. L. Rep. (BNA) 1310 (Sept. 12, 2011); Ute Krüdewagen & Lisa Stam, *Global Employee Terminations in the Age of Social Media*, LAW360 (Aug. 26, 2011), http://www.law360.com/articles/267702/global-employee-terminations-in-the-age-of-social-media.

[78] Heinisch v. Germany, App. No. 28274/08, Eur. Ct. H.R. (2011).

[79] Lothar Determann & Ute Krüdewagen, *Policing Social Media*, THE RECORDER, April 6, 2012, Katie W. Johnson, *Attorneys Encourage Companies to Adopt Social Media Guidelines for Employees*, 10 Privacy & Sec. L. Rep. (BNA) 1680 (Nov. 21, 2011).

[80] Lothar Determann, *Social Media @ Work—A Checklist for Global Businesses*, 11 Privacy & Sec. L. Rep. (BNA) 487 (Mar. 19, 2012).

[81] Erica Smith, *Too Much Worker, Application Personal Data, Too Little Understanding How to Handle It*, 10 Privacy & Sec. L. Rep. (BNA) 1591 (Nov. 7, 2011); *see also* Krüdewagen & Stam, *Global Recruitment and Social*

MYTH 12: CONSUMERS CARE ABOUT PRIVACY[83]

¶27 The U.S. Federal Trade Commission has publicly filed complaints and stated that the leading social media platform operators have handled their users' data in ways that harmed users by threatening their health and safety and potentially revealing their political views, sexual orientation, business relationships, and other sensitive information and affiliations to third parties without authorization.[84] The press reported extensively.[85] The providers apologized and settled the charges without putting up much of a defense.[86] They continue the push for more information sharing in the interest of expanding the reach of social networks and they continue innovating and expanding the commercialization of user data.[87] Meanwhile, active social media user numbers are reaching record highs: as of December 31, 2011, Facebook had 845 million monthly active users, a 39 percent increase as compared to the same figure a year earlier;[88] Twitter experienced a 182 percent increase in the number of its mobile users between early 2010 and early 2011, all while the average number of Tweets per day nearly tripled;[89] as of January 2012, Google+ amassed over 90 million registered users

---

Media Hiring Traps, LAW360 (Dec. 16, 2011), http://www.law360.com/articles/288802/global-recruitment-and-social-media-hiring-traps. Some employers have apparently even started asking candidates for their social media account passwords. *See California Bill Would Ban Demands for Worker, Job Applicant, Student Social Media Passwords*, 11 Privacy & Sec. L. Rep. (BNA) 600 (Apr. 2, 2012).

[82] European employers have to comply with significant restrictions on employee monitoring and investigations whereas U.S. employers can legitimize even very intrusive forms of monitoring by destroying employee privacy expectations with detailed notices (which may need to be updated to cover specific social media platforms). *See*, Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979 (2011).

[83] CENTER FOR DEMOCRACY & TECHNOLOGY, *Consumer Privacy*, *available at* https://www.cdt.org/issue/consumer-privacy (last visited Feb. 23, 2012) ("Privacy is the number one concern of Internet users; it is also the top reason why non-users still avoid the Internet."); Joseph Bonneau & Sören Preibusch, *The Privacy Jungle: On the Market for Data Protection in Social Networks*, THE EIGHTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2009), *available at* http://preibusch.de/publications/Bonneau_Preibusch__Privacy_Jungle__2009-05-26.pdf ("Given the plethora of competing sites, the functional similarity of most social networks, and users' stated concern for privacy, market conditions appear prime for sites to compete on the basis of privacy.").

[84] Complaint, Facebook, Inc., FTC File No. 092-3184 (Nov. 29, 2011); *see also* Complaint, Google, Inc., FTC File No. 102-3136 (Mar. 30, 2011) (alleging that the now defunct social networking service Google Buzz "did not adequately communicate that certain previously private information would be shared publicly by default," and that "the controls that would allow the user to change the defaults were confusing and difficult to find."); Complaint, Twitter, Inc., FTC File No. 092-3093 (June 24, 2010) (alleging that Twitter failed to provide reasonable and appropriate security to prevent unauthorized access to its users' private information).

[85] The press covered the FTC complaints and settlements extensively when the decisions were published in 2010 and 2011; for recent updates, see, for example, Lance Ulanoff, FTC: We've Protected the Privacy of a Billion People, May 31, 2012, http://mashable.com/2012/05/31/ftc-privacy; Mathew J. Schwartz, FTC Sets Consumer Data Collection Limits, http://www.informationweek.com/news/security/privacy/240002816; | Laurie Sullivan, Google, Facebook: Who's Tracking What?, Laurie Sullivan, Jun 14, 2012 (http://www.mediapost.com/publications/article/176828/google-facebook-whos-tracking-what.html#ixzz1zGjHW76d).

[86] *See* Mark Zuckerberg, *Our Commitment to the Facebook Community*, FACEBOOK BLOG (Nov. 29, 2011, 9:39am), http://blog.facebook.com/blog.php?post=10150378701937131 (Facebook CEO acknowledging that the company has made mistakes regarding its users' privacy and linking to the company's settlement with the FTC); Alma Whitten, *An update on Buzz*, OFFICIAL GOOGLE BLOG (Mar. 30, 2011, 7:30am), http://googleblog.blogspot.com/2011/03/update-on-buzz.html (Google Director of Privacy, Product & Engineering admitting that Google Buzz fell short of Google's usual standards for transparency and user control and let Google's users down); David Sarno, *FTC settles with Twitter on 'misleading' security practices*, L. A. TIMES BLOG (Mar. 11, 2011, 2:44pm), http://latimesblogs.latimes.com/technology/2011/03/ftc-settles-with-twitter-on-misleading-security-practices.html (noting that a Twitter spokeswoman's response to Twitter's settlement with the FTC entailed her pointing to a previous company blog post in which the company claimed it implemented many of the FTC's suggestions previously and that its agreement with the FTC formalized its commitment to those security practices).

[87] *See, e.g.*, April Dembosky, *Facebook Timeline ads plan raises fresh privacy fears*, FINANCIAL TIMES, Feb. 9, 2012, http://www.ft.com/cms/s/0/8e575f8e-529c-11e1-ae2c-00144feabdc0.html; *see also* Julia Angwin, *Google Widens Its Tracks, Privacy Changes to Combine Data on Users, Making Anonymity Harder to Keep*, WALL ST. J., Jan. 25, 2012, http://online.wsj.com/article/SB10001424052970203806504577181371465957162.html.

[88] U.S. Securities & Exchange Commission, Form S-1 Registration Statement for Facebook, Inc., Feb. 1, 2012, *available at* http://sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm.

[89] *#numbers*, TWITTER BLOG (Mar. 14, 2011, 11:38am), http://blog.twitter.com/2011/03/numbers.html.

since launching just half a year earlier.[90] The consumers have spoken: they are not concerned. People care more about getting free media than they do about their privacy.[91]

[90] Mark Milian, *Google Says Social Network Has 90M Users*, CNN TECH (Jan. 19, 2012), http://articles.cnn.com/2012-01-19/tech/tech_social-media_google-plus-users_1_search-engine-social-network-results-pages?_s=PM:TECH.

[91] April Dembosky, *supra* note 85 (quoting Rebecca Lieb, an analyst with the Altimeter Group).