No. 15-2560

IN THE
UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION, *et al.*,
PLAINTIFF-APPELLANTS,
v.

NATIONAL SECURITY AGENCY, *et al.*,
DEFENDANT-APPELLEES.

On Appeal From The United States District Court
For The District of Maryland
Baltimore Division
Case No. 5-cv-00662-TSE
Honorable Hon. T. S. Ellis, III, District Judge

BRIEF OF *AMICI CURIAE* COMPUTER SCIENTISTS AND TECHNOLOGISTS IN SUPPORT OF PLAINTIFF-APPELLANT WIKIMEDIA AND REVERSAL

Jennifer Stisa Granick
(CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Matthew J. Craig
Shapiro Arato LLP
500 Fifth Avenue, 40th Floor
New York, NY 10110
Telephone: (212) 257-4883
Facsimile: (212) 202-6417
mcraig@shapiroarato.com

Attorneys for *Amici Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

DISCLOSURE IN COMPLIANCE WITH FEDERAL RULE OF APPELLATE PROCEDURE 29(c)(5)

(A) No party's counsel authored this brief in whole or in part.

(B) No party or party's counsel contributed money to counsel for *amici curiae* or to any *amicus* that was intended to fund preparing or submitting this brief,

(C) No person—other than the *amicus curiae*, its members, or its counsel—contributed money that was intended to fund preparing or submitting this brief.

CONSENT OF PARTIES TO FILING

All parties have consented to the filing of this brief, via attorney Alexander Abdo on behalf of Plaintiff-Appellants Wikimedia Foundation *et al*. and attorney Catherine Hancock Dorsey, Appellate Staff Civil Division, U.S. Department of Justice on behalf of Defendants-Appellees National Security Agency *et al*.

STATEMENT OF INTEREST

The parties listed in Exhibit A submit this brief as *amici curiae*. *Amici* are an illustrious group of computer scientists, computer science professors, technologists, internet networking experts, and academics with diverse expertise on the science and practice of internet networking, and content scanning for the purposes of spam filtering, copyright interdiction, and network security. ***Amici* sign in their personal capacity, and titles and employer affiliations are provided for identification purposes only.**

Amici include Bruce Schneier, an internationally renowned security technologist, called a "security guru" by The Economist. Schneier is a fellow at the Berkman Center for Internet and Society at Harvard University, a board member of the Electronic Frontier Foundation, and an Advisory Board member of the Electronic Privacy Information Center. He is also the Chief Technology Officer of Resilient Systems, Inc.

Also joining the brief is Dr. Nicholas Weaver, a Researcher at the International Computer Science Institute. The Networking and Security Group focuses on understanding the behavior, use, and abuse of today's Internet, and on exploring new technology, designs, and defenses for tomorrow's Internet. Dr. Weaver's research focus is on network security, notably worms, botnets, and other internet-scale attacks, and network measurement.

ARGUMENT

This lawsuit presents a constitutional challenge to the U.S. government's "Upstream" surveillance program. Plaintiffs allege that the government is copying and reviewing substantially all international text-based communications, including their own, and that they have established to a virtual certainty that the government is copying and reviewing at least some of their communications. The District Court dismissed the case for lack of standing, opining that Plaintiffs' allegations were based on speculation and conjecture.

As technical experts, we disagree. The information publicly available about the Upstream program, combined with an understanding of how the internet works, leads to the inevitable conclusion that the NSA is copying and searching all communications that flow through the particular points on the internet "backbone" at which the NSA has intervened. All international communications travel through a limited number of international internet links, or circuits, on this backbone. The government has officially acknowledged monitoring multiple circuits. Plaintiff Wikimedia's international communications traverse every one of these circuits. Finally, the NSA seizes and searches all communications that travel over each circuit that it is monitoring.

Therefore, it is certain, as a technical matter, that some of Plaintiff Wikimedia's communications have been subject to Upstream surveillance. For this

reason, the District Court decision should be reversed, and this lawsuit should be allowed to proceed.[1]

I. A Brief Legal History Of Upstream Surveillance

Following the terrorist attacks of September 11, 2001, President Bush authorized a secret surveillance program aimed at collecting communications thought to contain foreign intelligence information when one end of the communication was in the United States. Many companies, including AT&T, voluntarily cooperated with this surveillance program. In 2005, after the press revealed the existence of the warrantless wiretapping portions of the program, the government sought to place it on surer legal footing. These efforts eventually led to the enactment of the FISA Amendments Act in 2008.

Section 702 of the FISA Amendments Act provided a statutory framework for programmatic surveillance of foreign targets without probable cause, even when they communicated with people within the United States. In other words, the purpose and function of Section 702 is to enable surveillance of foreigners overseas who are communicating with U.S. persons such as Plaintiffs. Section 702 also empowered the government to *compel*, not just request, cooperation from service providers.

---

[1] Plaintiffs rely on two distinct standing theories. See Pl. Br. Sections I.B-C. Both of those standing claims are plausible. For the purposes of this brief, however, amici focus their technological analysis on Plaintiff Wikimedia's standing claim.

For years, the public's understanding of Section 702 was confined to the text of the statute itself. In a previous legal challenge to the statute, the Supreme Court observed that without facts about how the government had implemented Section 702, it was not clear whether the government had engaged in broad surveillance, let alone that such surveillance touched the particular plaintiffs in that case. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1148 (2013). For those reasons and others, the Court dismissed that challenge for lack of standing.

Much has changed since then. As a result of public disclosures regarding NSA surveillance, the publication of comprehensive government reports, and the declassification of multiple FISC opinions, the public's legal and technical understanding of Section 702 surveillance has increased substantially.

Importantly, it is now clear that the NSA uses Section 702 to compel communications providers to assist with surveillance of the internet "backbone"—the high-capacity cables, switches, and routers that route both domestic and international communication via the internet. *See* Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("PCLOB Report") 35-37 (2014); Am. Compl. ("Compl.") ¶¶ 40-47 (JA 40-43). This backbone surveillance—called Upstream surveillance by the government—enables the NSA to capture communications to, from, and even about foreign intelligence targets.

II. The NSA Monitors Internet Circuits Through Which Plaintiff Wikimedia's Communications Flow

Through Upstream surveillance, the NSA wiretaps communications directly from the internet backbone with the compelled assistance of the telecommunications companies that control the relevant access points. Because Upstream surveillance captures internet communications in transit, the mode by which data moves across the internet backbone has important implications for how Upstream surveillance functions.

Although the internet is largely decentralized, there are network chokepoints on the internet backbone that handle a substantial amount of data. There are 49 high-capacity submarine cables that enter the United States at 43 different locations, through which virtually all communications entering or leaving the United States flow. *See* TeleGeography Submarine Cable Map, available at http://www.submarinecablemap.com/#/country/united-states. (While 65 undersea cables touch down in the U.S., 49 of them are international, and those collectively use 43 landing points.) In addition, there are a limited number of high-capacity cables that link major metropolitan areas in the United States. Surveillance conducted at these chokepoints gives a wiretapper access to huge amounts of international internet communications. Domestic communications traverse these chokepoints as well.

The NSA conducts Upstream surveillance using surveillance devices installed on the internet backbone. Compl. ¶ 47 (JA 42-43).[2] These surveillance devices are located at chokepoints through which flow almost all internet communications entering or leaving the country. *Id.* ¶¶ 60, 68-69 (JA 47, 50-51). The government has acknowledged that it conducts Upstream surveillance on these major internet circuits. *See* [Redacted], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011) (The NSA collects communications transactions when "routed through an international internet link being monitored by NSA"); David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions 2d* § 16.12 n.10, § 17.5 n.49 (Database updated July 2015) ("The government's December 2014 disclosures confirm that large facilities, carrying communications from many individual telephone numbers and e-mail addresses, were surveilled."); *see also* PCLOB Report at 36-37; Compl. ¶¶ 68-69 (JA 50-51). And published documents from the NSA show that just one telecommunications provider gives the NSA

[2] Some of the steps involved in Upstream surveillance may be performed by telecommunications providers. *See* Am. Compl. ¶¶ 47-49 (stating that some aspects of Upstream surveillance may be conducted by telecommunications providers at the government's behest); PCLOB Report at 7, 32. Regardless of whether the NSA or the provider conducts the collection, it is performed at the government's behest and pursuant to Section 702, and therefore constitutes government action.

Upstream surveillance capabilities at seven major international facilities. Compl. ¶ 68 (JA 50-51).[3]

As Plaintiffs explain, Wikimedia operates one of the ten most-visited websites in the world and engages in more than a trillion international internet communications each year. Compl. ¶ 88 (JA 56). Wikimedia has hundreds of millions of users, who are located in virtually every country on Earth. *Id*. ¶¶ 79, 85 (JA 53, 55). Wikimedia's trillion-plus international communications are so numerous and so widely distributed across the internet, its communications traverse every major internet circuit entering or leaving the United States. Id. ¶ 61 (JA 48).

For an entity like Wikimedia, given their volume of internet traffic, it would be impossible that none of their communications travelled through one of the international circuits the NSA monitors. This inevitability holds, even if one believes the improbable claim that the NSA only monitors a few international circuits. *See* District Court Opinion at 17 (JA 190) (citing "the fact that Upstream surveillance equipment has been installed at some of the Internet backbone chokepoints.") With over a trillion international communications per year, it is

[3] It stands to reason that the NSA has many more circuits tapped. Nevertheless, the analysis that follows holds even if the Court were to assume that the NSA has intervened at just one point on the internet backbone.

virtually certain that Wikimedia communications have passed through a NSA monitored circuit, even if the NSA is monitoring just one.

III. Upstream Necessarily Involves Searching *All* Communications That Traverse Circuits On The Internet Backbone At Which the NSA Or Its Agents Have Installed Surveillance Equipment

It is also certain that when Wikimedia's communications pass through the NSA monitored circuit or circuits, the government seizes and searches them. This is not speculation. Technological realities make it clear that the NSA seizes and searches every communication that passes through the monitored circuits on the internet backbone. The only technologically feasible way for Upstream surveillance to work is for the NSA to seize the entire flow of internet communications *content* flowing over a particular circuit on the internet backbone, and only after this seizure, search all non-filtered packets for selectors.

After copying the data that flows through a monitored circuit, the NSA first attempts to filter purely domestic communications out of the captured data. As the government has acknowledged, however, this filtering process is imperfect. Many purely domestic communications are routed internationally, while others are bundled with international communications and thus will not be eliminated through filtering. Importantly, the NSA makes no attempt to filter out a U.S. person's communications with a non-U.S. person outside of the United States, as Section 702 expressly permits surveillance of such communications.

The NSA also attempts to filter out certain types of uninteresting internet traffic, such as streaming movies. The NSA does not filter out http (World Wide Web) traffic generally and has even identified Wikimedia traffic as an example of information in which it is specifically interested. Compl. ¶ 107 (JA 63).

Next, the NSA searches the non-filtered data using "selectors." A designated selector could be an email address associated with a foreign intelligence target or some other selector believed to reflect a foreign intelligence purpose. Kris & Wilson, *National Security Investigations & Prosecutions 2d* § 17.5. The NSA retains those communications containing its selectors for further analysis and distribution.

Importantly, Upstream surveillance does not involve the NSA's seizure and search of only the communications that contain selectors. That is because, in order to determine whether a particular communication contains a selector, the government must seize and search all of the communications transiting the circuit it is monitoring. At the time that the communication goes through the NSA monitoring equipment, the government has no idea whether or not it contains the relevant selector. Only by seizing and then searching every communication that passes through its devices can the NSA determine which communications contain its selectors. See [Redacted], 2011 WL 10945618 at *14 ("[A]t the time of acquisition, the NSA's upstream collection devices often lack the capability to

determine whether a transaction contains a single communication or multiple communications, or to identify the parties to any particular communication within a transaction.").

The basic architecture of the internet explains why. The internet is a "packet switched" network, meaning that, unlike the telephone network which directly connects the individuals speaking to each other, the internet breaks all digital communications into "packets"—discrete chunks of information that are relatively small. Packets are labeled with important routing information, including the origin and destination internet protocol address, or IP address. The IP address tells intermediary computers where to send information, and packets travel from machine to machine (and network to network) until the information reaches its destination.

Most internet communications will constitute more than one packet, as packets are commonly less than 1500 bytes in size. Center for Applied Internet Data Analysis, *Packet size distribution comparison between Internet links in 1998 and 2008* (Jan. 14, 2010), https://www.caida.org/research/traffic-analysis/pkt_size_distribution/graphs.xml. A typical webpage such as those communicated by Plaintiff Wikimedia is multiple times that size. For example, the Wikipedia page for attorney Jennifer Granick constitutes 110,767 bytes, which means that it might traverse the internet in 70 packets or more. *See Jennifer*

Granick, Wikipedia, https://en.wikipedia.org/wiki/Jennifer_Granick (last visited Feb. 22, 2016). Because a single communication is often broken into multiple packets, packets are also labeled with information that allows destination computers to reassemble multiple constituent packets back into a single, readable communication.

The information of potential interest to the NSA is contained within the part of an internet packet known as the "Application Layer." The Application Layer contains the actual content of the communication being transmitted. In order to determine which communications contain its selectors, the NSA must first seize and then search the content—i.e., the Application Layer—of each packet that flows across the particular points of the internet backbone at which it has intervened. There is no other way the NSA knows whether a particular packet contains a particular selector. As a result, Upstream surveillance can be understood as the internet equivalent of opening and reading all mail passing through the post office in order to determine whether letters concern foreign intelligence targets. *See* Kris & Wilson, *National Security Investigations & Prosecutions 2d* § 17.5 ("NSA's machines scan the contents of all of the communications passing through the collection point . . .").

The NSA's acknowledgement of "about" surveillance confirms that Upstream surveillance involves searching the contents of all packets that pass

through the NSA's points of interception. "About" surveillance refers to the collection of communications that are not to or from a particular selector, but rather mention—i.e., are about—that selector. For instance, if the NSA's designated selector were an email address, the only way the agency would know that a web page or other http connection to Wikimedia contained that email address as part of a Wikipedia web page, suggested edit, or chat room is for the NSA to search the content of the non-filtered packets that pass through the surveillance devices.

The fact that a single communication is typically too large to fit into a single packet only further illustrates why Upstream surveillance necessarily involves seizing and then searching *every* internet packet that flows through the NSA collection devices on the internet backbone, regardless of whether that communication is of foreign intelligence relevance or not. When the content of a single communication is too large to fit into a single packet, that communication will be divided into multiple packets. These packets will travel across the internet backbone and independently arrive at a single destination, where they will be reassembled so that the recipient can receive and "read" the message being sent—whether an email, instant message, webpage, or video.

Because a communication traverses the internet backbone as separate packets traveling at different times, the NSA must capture all data that passes

through its points of interception in order to reassemble the packets into a comprehensible communication. This is not speculation, this is common networking sense.

Imagine a short email that is split into three packets. Only the third packet contains the NSA selector BadGuy@example.com. Upon identifying the selector in the third packet, the NSA can only reassemble the communication if it has at least temporarily seized the first two packets that make up the communication. Only then may the three packets be joined together into a readable message. Without at least temporarily storing the packets comprising the internet flow, the NSA cannot be sure that it will have all the packets comprising a message it wants to collect.[4] Otherwise, when the packet containing an NSA selector arrives after the other packets comprising the same message, the NSA will be unable to reassemble the message and make sense of it. The meaning of intercepted foreign intelligence communications would be lost.

---

[4] Defendants relied on the Declaration of Robert Lee below in order to dispute Plaintiffs' allegations on the merits. Mr. Lee asserted that "not all packets of a given TCP stream are necessary to intelligibly assemble its contents." Decl. of Robert T. Lee ("Lee Decl.") ¶ 13 n.4 (JA 107). Lee explains that "each TCP stream includes packets that do not transmit substantive information but that facilitate the connection." *Id*. The fact that TCP streams include some packets that do not contain communications content (e.g. TCP's "three way handshake"—packets that request to open a connection, acknowledge receipt of that request, and then acknowledge that the second transmission was received by the initiating device, *id*.) does not refute our point that the government must collect those packets that do contain content in order to make sense of the reassembled message later on.

For these reasons, Upstream collection necessarily entails seizing and searching the contents of every non-filtered international communication that flows through a circuit that the NSA monitors.

IV. Plaintiffs' Allegations That Their Communications Have Been Seized And Searched As Part of the Government's Upstream Surveillance Program Are Based On Technological Facts, and Not Mere Speculation

The principal question before this Court is whether Wikimedia and other Plaintiffs have plausibly alleged that they face a "substantial risk" that the NSA has searched their communications under the Upstream surveillance program. *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). A complaint should not be dismissed if it is "plausible" and "provides sufficient detail about the claim to show that the plaintiff has a more-than-conceivable chance of success on the merits." *Goldfarb v. Mayor & City Council of Balt.*, 791 F.3d 500, 511 (4th Cir. 2015). From a technological perspective, the allegation that Plaintiffs communications have been seized and searched by Defendants is more than plausible. Especially with regard to Plaintiff Wikimedia, the facts now known about Upstream surveillance, coupled with a basic understanding of the way the internet works, renders any other inference simply unfathomable. Wikimedia's communications travel internationally over every internet circuit. The NSA monitors one or more of those circuits. That monitoring consists of seizing, searching, and potentially

ingesting Wikimedia messages into NSA databases. This allegation is not just plausible, it is highly credible.

Wikimedia's communications permeate the international internet circuits, and the NSA is there. Wikimedia's trillion communications per year transit every major internet circuit entering or leaving the United States. As a result, the government need only be monitoring one such circuit—and its own acknowledgements make clear it is doing so—in order to encounter Wikimedia communications. When conducting Upstream surveillance, the government is copying and searching all the international text-based communications on each of the circuits it is monitoring. Just as a chef ingests salt when she tastes a seasoned pot of soup, the NSA searches Wikimedia communications when it monitors one or more international internet circuits.

Wikimedia is challenging the constitutionality of that seizure and search. *Amici* express no opinion on that underlying matter. But we do believe that Wikimedia has alleged sufficient facts to show standing to bring this case.

CONCLUSION

For the reasons above, *amici* submit that this Court should reverse the District Court ruling dismissing the case.

Dated: February 24, 2016

By: /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Matthew J. Craig
Shapiro Arato LLP
500 Fifth Avenue, 40th Floor
New York, NY 10110
Telephone: (212) 257-4883
Facsimile: (212) 202-6417
mcraig@shapiroarato.com

Attorneys for *Amici Curiae*

APPENDIX A
List of *Amici Curiae*

- Katherine Carpenter, J.D. M.A.: Privacy, Data Security, and Health Consultant
- Roger Dingledine, The Tor Project
- Mike Doherty, Systems Engineer, Google
- Dr. Stephen Farrell, Trinity College, Dublin
- Dan Farmer, CSO, MultiScale Health Networks
- Jim Fenton, Independent Internet Technologist
- Dr. Richard Forno, Jr Affiliate Scholar, Stanford Law School Center for Internet and Society
- Christopher Gilbert, Senior Application Developer
- J. Alex Halderman: Associate Professor of Computer Science and Engineering and Director, Center for Computer Security and Society, University of Michigan
- Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology
- Ted Hardie, Member, Internet Architecture Board
- Dan Kaminsky, Chief Scientist, White Ops
- Barry Leiba, IETF Applications and Real-Time Area Director
- Patrick R. McDonald, Technical Program Manager

Amici sign in their personal capacity, and the following titles and employer affiliations are provided for identification purposes only.

- Bruce Schneier, Fellow, Berkman Center for Internet and Society at Harvard University and CTO Resilient Systems, Inc.

- Tim Skorick, Technical Lead, Threat and Vulnerability Management, Americas, Hewlett Packard Enterprise

- Brian Trammell, Senior Researcher, Swiss Federal Institute of Technology (ETH) Zurich; and Member, Internet Architecture Board

- Nick Sullivan, Head of Cryptography, CloudFlare Inc.

- Brett Thomas, CTO, Vindicia

- Nicholas Weaver, Researcher, International Computer Science Institute

- Michael J. Young, CISSP CISM CISA, Board Member, New York Information Systems Security Association, US and International Board Adviser, Information Systems Security Association

Amici sign in their personal capacity, and the following titles and employer affiliations are provided for identification purposes only.

CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amici Curiae* In Support Of Plaintiffs-Appellants complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 3,253 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point Times.

Dated: February 24, 2016

By: /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society

Matthew J. Craig
Shapiro Arato LLP

Attorneys for *Amici Curiae*

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system on February 24, 2016.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: February 24, 2016

By: /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Matthew J. Craig
Shapiro Arato LLP
500 Fifth Avenue, 40th Floor
New York, NY 10110
Telephone: (212) 257-4883
Facsimile: (212) 202-6417
mcraig@shapiroarato.com

Attorneys for *Amici Curiae*