UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION
149 New Montgomery Street, 6th Floor
San Francisco, CA 94105;

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1660 L Street, NW, 12th Floor
Washington, DC 20036;

HUMAN RIGHTS WATCH
350 Fifth Avenue, 34th Floor
New York, NY 10118;

AMNESTY INTERNATIONAL USA
5 Pennsylvania Plaza, 16th Floor
New York, NY 10001;

PEN AMERICAN CENTER
588 Broadway, Suite 303
New York, NY 10012;

GLOBAL FUND FOR WOMEN
222 Sutter Street, Suite 500
San Francisco, CA 94108;

THE NATION MAGAZINE
33 Irving Place, 8th Floor
New York, NY 10003;

THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, VA 22906;

WASHINGTON OFFICE ON LATIN AMERICA
1666 Connecticut Avenue, NW, Suite 400
Washington, DC 20009,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE

FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Civil Action No.
15-cv-00662-TSE

Hon. T. S. Ellis, III

9800 Savage Road
Fort Meade, Anne Arundel County, MD 20755;

ADM. MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service,
National Security Agency / Central Security Service
9800 Savage Road
Fort Meade, Anne Arundel County, MD 20755;

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Washington, DC 20511;

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence,
Office of the Director of National Intelligence
Washington, DC 20511;

DEPARTMENT OF JUSTICE
950 Pennsylvania Avenue, NW
Washington, DC 20530;

LORETTA E. LYNCH, in her official capacity as Attorney General of the United States,
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530,

Defendants.

Deborah A. Jeon
(Bar No. 06905)
jeon@aclu-md.org
David R. Rocah
(Bar No. 27315)
rocah@aclu-md.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

Patrick Toomey
(pro hac vice)
ptoomey@aclu.org
Jameel Jaffer
(pro hac vice)
jjaffer@aclu.org
Alex Abdo
(pro hac vice)
aabdo@aclu.org
Ashley Gorski
(pro hac vice)
agorski@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

Charles S. Sims
(pro hac vice)
csims@proskauer.com
David A. Munkittrick
(pro hac vice)
dmunkittrick@proskauer.com
John M. Browning
(pro hac vice)
jbrowning@proskauer.com
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900

June 19, 2015

FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. This lawsuit challenges the suspicionless seizure and searching of internet traffic by the National Security Agency ("NSA") on U.S. soil. The NSA conducts this surveillance, called "Upstream" surveillance, by tapping directly into the internet backbone inside the United States—the network of high-capacity cables, switches, and routers that today carry vast numbers of Americans' communications with each other and with the rest of the world. In the course of this surveillance, the NSA is seizing Americans' communications en masse while they are in transit, and it is searching the contents of substantially all international text-based communications—and many domestic communications as well—for tens of thousands of search terms. The surveillance exceeds the scope of the authority that Congress provided in the FISA Amendments Act of 2008 ("FAA") and violates the First and Fourth Amendments. Because it is predicated on programmatic surveillance orders issued by the Foreign Intelligence Surveillance Court ("FISC") in the absence of any case or controversy, the surveillance also violates Article III of the Constitution.

2. Plaintiffs are educational, legal, human rights, and media organizations that collectively engage in more than a trillion sensitive international communications over the internet each year. Plaintiffs communicate with, among many others, journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses. Plaintiff Wikimedia Foundation communicates with the hundreds of millions of individuals who visit Wikipedia webpages to read or contribute to the vast repository of human knowledge that Wikimedia maintains online. The ability to exchange information in confidence, free from warrantless government monitoring, is essential to each of

the Plaintiffs' work. The challenged surveillance violates Plaintiffs' privacy and undermines their ability to carry out activities crucial to their missions.

3. Plaintiffs respectfully request that the Court declare the government's Upstream surveillance to be unlawful; enjoin the government from continuing to conduct Upstream surveillance of Plaintiffs' communications; and require the government to purge from its databases all of Plaintiffs' communications that Upstream surveillance has already allowed the government to obtain.

JURISDICTION AND VENUE

4. This case arises under the Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the Constitution and 28 U.S.C. § 1331. The Court also has jurisdiction under the Administrative Procedure Act, 5 U.S.C. § 702. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202. The Court has authority to award costs and attorneys' fees under 28 U.S.C. § 2412.

5. Venue is proper in this district under 28 U.S.C. § 1391(b)(2), (e)(1).

PLAINTIFFS

6. Wikimedia Foundation ("Wikimedia") is a non-profit organization based in San Francisco, California, that operates twelve free-knowledge projects on the internet. Wikimedia's mission is to empower people around the world to collect and develop free educational content. Wikimedia does this by developing and maintaining "wiki"-based projects, and by providing the full contents of those projects to individuals around the world free of charge. Wikimedia sues on its own behalf and on behalf of its staff and users.

7. The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C. NACDL advocates for rational and humane criminal justice policies at all levels of federal, state, and local government, and seeks to foster the integrity, independence, and expertise of the criminal defense profession. NACDL sues on its own behalf and on behalf of its members.

8. Human Rights Watch ("HRW") is a non-profit, non-governmental human rights organization headquartered in New York City with offices around the world. It reports on abuses in all regions of the globe and advocates for the protection of human rights. HRW researchers conduct fact-finding investigations into human rights abuses in over 90 countries and publish their findings in hundreds of reports, multi-media products, and other documents every year, as well as through social media accounts. HRW sues on its own behalf and on behalf of its staff.

9. Amnesty International USA ("AIUSA"), headquartered in New York City, is the largest country section of Amnesty International, with hundreds of thousands of members and other supporters who work for human rights, including through national online networks, high schools, colleges, and community groups. AIUSA sues on its own behalf and on behalf of its staff and members.

10. PEN American Center ("PEN") is a human rights and literary association based in New York City. Committed to the advancement of literature and the unimpeded flow of ideas and information, PEN fights for freedom of expression; advocates on behalf of writers harassed, imprisoned, and sometimes killed for their views; and fosters international exchanges, dialogues, discussions, and debates. PEN sues on its own behalf and on behalf of its staff and members.

11. Global Fund for Women ("GFW") is a non-profit grantmaking foundation based in San Francisco, California, and New York City. GFW advances women's human rights worldwide by providing funds to women-led organizations that promote the economic security, health, safety, education, and leadership of women and girls. GFW sues on its own behalf and on behalf of its staff.

12. The Nation Magazine ("The Nation"), which is published by The Nation Company, LLC, and based in New York City, is America's oldest weekly magazine of opinion, news, and culture. It serves as a critical, independent voice in American journalism, exposing abuses of power through its investigative reporting, analysis, and commentary. In recent years, The Nation's journalists have reported on a wide range of issues relating to international affairs, including the wars in Iraq and Afghanistan, the Israel–Palestine conflict, protest activities in China and elsewhere in East Asia, and conflicts in Africa and Latin America. The Nation sues on behalf of itself, its staff, and certain of its contributing journalists.

13. The Rutherford Institute ("Rutherford") is a civil liberties organization based in Charlottesville, Virginia, committed to protecting the constitutional freedoms of Americans and the human rights of all people. Rutherford provides free legal services in defense of civil liberties and educates the public about constitutional and human rights issues. It also advocates on behalf of individuals abroad whose rights are threatened by foreign governments. Rutherford sues on its own behalf and on behalf of its staff.

14. The Washington Office on Latin America ("WOLA") is a non-profit, non-governmental organization based in Washington, D.C., that conducts research, advocacy, and education designed to advance human rights and social justice in the Americas. WOLA sues on its own behalf and on behalf of its staff.

DEFENDANTS

15. Defendant National Security Agency / Central Security Service ("NSA"), headquartered in Fort Meade, Maryland, is the agency of the United States government responsible for conducting the surveillance challenged in this case.

16. Defendant Adm. Michael S. Rogers is the Director of the NSA and the Chief of the Central Security Service. Defendant Rogers is sued in his official capacity.

17. Defendant Office of the Director of National Intelligence ("ODNI") is the agency of the United States government responsible for directing and coordinating the activities of the intelligence community, including the NSA.

18. Defendant James R. Clapper is the Director of National Intelligence ("DNI"). Together with the Attorney General, the DNI authorizes warrantless surveillance of U.S. citizens' and residents' international communications under the FAA, including Upstream surveillance. Defendant Clapper is sued in his official capacity.

19. Defendant Department of Justice ("DOJ") is one of the agencies of the United States government responsible for authorizing and overseeing surveillance conducted pursuant to the FAA, including Upstream surveillance.

20. Defendant Loretta E. Lynch is the Attorney General of the United States. Together with the DNI, the Attorney General authorizes warrantless surveillance of U.S. citizens' and residents' international communications under the FAA, including Upstream surveillance. Defendant Lynch is sued in her official capacity.

LEGAL AND FACTUAL BACKGROUND

The Foreign Intelligence Surveillance Act

21. In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") to govern surveillance conducted for foreign intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC") and empowered the court to grant or deny government applications for surveillance orders in certain foreign intelligence investigations.

22. Congress enacted FISA after years of in-depth congressional investigation by the committees chaired by Senator Frank Church and Representative Otis Pike, which revealed that the Executive Branch had engaged in widespread warrantless surveillance of United States citizens—including journalists, activists, and members of Congress—"who engaged in no criminal activity and who posed no genuine threat to the national security."

23. Congress has amended FISA multiple times since 1978.

24. Prior to 2007, FISA generally required the government to obtain an individualized order from the FISC before conducting electronic surveillance on U.S. soil. To obtain a traditional FISA order, the government was required to make a detailed factual showing with respect to both the target of the surveillance and the specific communications facility—often a telephone line or email account—to be monitored. The government was also required to certify that a "significant purpose" of the surveillance was to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(6)(B).

25. The FISC could issue such an order only if it found, among other things, that there was probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that "each of the facilities or places at which the

electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2)(A)–(B).

26. The framework established by FISA remains in effect today, but it has been modified by the FAA to permit the acquisition of U.S. citizens' and residents' international communications without probable cause or individualized suspicion, as described below.

The Warrantless Wiretapping Program

27. On October 4, 2001, President George W. Bush secretly authorized the NSA to conduct a program of warrantless electronic surveillance inside the United States. This program, which was known as the President's Surveillance Program ("PSP"), was reauthorized repeatedly by President Bush between 2001 and 2007.

28. According to public statements by senior government officials, the PSP involved the warrantless interception of emails and telephone calls that originated or terminated inside the U.S. According to then-Attorney General Alberto Gonzales and then-NSA Director General Michael Hayden, NSA "shift supervisors" initiated surveillance when in their judgment there was a "reasonable basis to conclude that one party to the communication [was] a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."

29. On January 17, 2007, then-Attorney General Alberto Gonzales publicly announced that a judge of the FISC had "issued orders authorizing the Government to target for collection international communications into or out of the United States where there [was] probable cause to believe that one of the communicants [was] a member or agent of al Qaeda or an associated terrorist organization." The Attorney General further stated that "[a]s a result of

these orders, any electronic surveillance that was occurring" as part of the PSP would thereafter "be conducted subject to the approval of the Foreign Intelligence Surveillance Court."

30. In April 2007, when the government sought reauthorization of the FISC's previous orders, a different judge of the FISC determined that key elements of the government's request were incompatible with FISA. Following the FISC's refusal to renew certain portions of its January 2007 orders, executive-branch officials appealed to Congress to amend the statute.

The Protect America Act

31. Congress enacted the Protect America Act ("PAA") in August 2007. The PAA expanded the executive's surveillance authority and provided legislative sanction for surveillance that the President had previously been conducting under the PSP. Because of a "sunset" provision, the amendments to FISA made by the PAA expired on February 17, 2008.

The FISA Amendments Act

32. President Bush signed the FISA Amendments Act ("FAA") into law on July 10, 2008. The FAA radically revised the FISA regime that had been in place since 1978 by authorizing the acquisition without individualized suspicion of a wide swath of communications, including U.S. persons' international communications, from companies inside the United States.[1]

33. In particular, the FAA allows the Attorney General and Director of National Intelligence to "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence

[1] Plaintiffs use the term "international" to describe communications that either originate or terminate outside the United States, but not both—*i.e.*, communications that are foreign at one end.

information." 50 U.S.C. § 1881a(a). The statute requires the Attorney General, in consultation with the Director of National Intelligence, to adopt "targeting procedures" and "minimization procedures," *id.* § 1881a(d)–(e), that govern who may be targeted for surveillance by executive-branch employees and how communications are to be handled once intercepted.

34. The FISC's role in overseeing the government's surveillance under the statute consists principally of reviewing these general procedures. The FISC never reviews or approves the government's individual surveillance targets or the facilities it intends to monitor. Rather, when the government wishes to conduct surveillance under the statute, it must certify to the FISC that the court has approved its targeting and minimization procedures or that it will shortly submit such procedures for the FISC's approval. *See id.* § 1881a(g), (i). If the government so certifies, the FISC authorizes the government's surveillance for up to a year at a time. A single such order may result in the acquisition of the communications of thousands of individuals.

35. The effect of the FAA is to give the government sweeping authority to conduct warrantless surveillance of U.S. persons' international communications. While the statute prohibits the government from intentionally *targeting* U.S. persons, it authorizes the government to acquire U.S. persons' communications with the foreigners whom the NSA chooses to target. Moreover the statute does not meaningfully restrict *which* foreigners the government may target. The statute does not require the government to make any finding—let alone demonstrate probable cause to the FISC—that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. The government may target any person for surveillance if it has a reasonable belief that she is a foreigner outside the United States who is likely to communicate "foreign intelligence information"—a term that is

defined so broadly as to encompass virtually any information relating to the foreign affairs of the United States. *Id.* §§ 1881a(a), 1801(e). The government may target corporations and associations under the same standard.

36. Thus, though the FAA is nominally concerned with the surveillance of individuals and groups outside the United States, it has far-reaching implications for U.S. persons' privacy. The targets of FAA surveillance may include journalists, academic researchers, human rights defenders, aid workers, business persons, and others who are not suspected of any wrongdoing. In the course of FAA surveillance, the government may acquire the communications of U.S. citizens and residents with all these persons.

THE GOVERNMENT'S IMPLEMENTATION OF THE FAA

37. The government has implemented the FAA expansively, with significant consequences for Americans' privacy. The Director of National Intelligence has reported that, in 2014, the government relied on the FAA to target 92,707 individuals, groups, or organizations for surveillance under a single court order. According to the FISC, the government gathered 250 million internet communications under the FAA in 2011 alone—at a time when the NSA had far fewer targets than it has today. Moreover, as described below, that figure does not reflect the far greater number of communications that the NSA searched for references to its targets before discarding them. Intelligence officials have declined to determine, or even estimate, how many of the communications intercepted under the FAA are to, from, or about U.S. citizens or residents. However, opinions issued by the FISC, reports by the President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board, and media accounts indicate that FAA

surveillance results in the wide-ranging and persistent interception of U.S. persons' communications.

38. In at least one respect, the government has engaged in surveillance that exceeds even the broad authority that Congress granted in the FAA. As described below, the government has interpreted the FAA to allow it to intercept, copy, and review essentially everyone's internet communications in order to search for identifiers associated with its targets. This intrusive and far-reaching practice has no basis in the statute. The statute authorizes surveillance only of *targets'* communications; it does not authorize surveillance of everyone.

Upstream Surveillance of Internet Communications

39. The government conducts at least two kinds of surveillance under the FAA. Under a program called "PRISM," the government obtains stored and real-time communications directly from U.S. companies—such as Google, Yahoo, Facebook, and Microsoft—that provide communications services to targeted accounts.

40. This case concerns a second form of surveillance, called Upstream. Upstream surveillance involves the NSA's seizing and searching the internet communications of U.S. citizens and residents en masse as those communications travel across the internet "backbone" in the United States. The internet backbone is the network of high-capacity cables, switches, and routers that facilitates both domestic and international communication via the internet.

Background: Internet Communications

41. The internet is a global network of networks. It allows machines of different types to communicate with each other through a set of intermediating networks. At its most basic level, it consists of (1) computers and the connections between them, (2) the

communications transmitted to, by, or through those computers and connections, and (3) the rules that direct the flow of these communications.

42. All communications on the internet are broken into "packets"—discrete chunks of information that are relatively small. The packets are sent from machine to machine (and network to network) and may traverse a variety of physical circuits connecting different machines before reaching their destination. Once the packets that make up a particular communication reach their final destination, they are reassembled so that the recipient can "read" the message being sent—whether an email, a webpage, or a video.

43. Internet packets can be thought of in layers. Although computer scientists describe these layers differently depending on the context, there are three layers relevant here:

- **The Networking Layer:** The Networking Layer of a packet is like an address block on an envelope. It contains, among other things, the packet's source and destination addresses. On the internet, addresses are represented as numeric strings known as Internet Protocol ("IP") addresses. To send a packet from one IP address to another, a computer on the internet creates a packet, addresses the packet with the source and destination IP addresses, and then transmits the packet to a neighboring computer that is closer to the destination. That computer then transmits the packet to another that is closer still to the destination. This process continues until the packet reaches its destination.

- **The Transport Layer:** The Transport Layer of a packet contains information that allows it to be grouped with other packets that are part of the same session or class of communication. For example, a packet sent using the most common Transport Layer protocol (the Transmission Control Protocol ("TCP")) contains, among other things, (1) a sequence number, which allows the recipient to reassemble the packets of a communication in order, and (2) source and destination "ports," which are, in effect, internal addresses used by the sending and receiving computers.

- **The Application Layer:** The Application Layer of a packet is akin to the inside of an envelope—it contains the actual content of the communications being transmitted. If the content is too large to fit into a single packet, then the Application Layers of several different packets would need to be reassembled in order for the recipient to be able to read or interpret the communication. For example, HTTP is the Application Layer protocol used to transmit webpages. Because most websites exceed the size of a single internet packet, their contents are transmitted in a series of HTTP packets that must be reassembled before display. Other common Application Layer protocols that, like

> HTTP, contain text-searchable data are SMTP (for the sending of email), IMAP and POP (for the receiving of email), and DNS (which allows computers to learn a website's IP address based on its domain name).

44. In some cases, internet packets stay on a single network (e.g., two machines in the same office talking to each other), but in other cases, the packets may traverse dozens of intermediate networks before reaching their destination. The network path can change radically and dynamically as devices and connections are added or removed from the network.

45. Often, there are multiple routes that an internet packet could follow to reach its destination. Some connected networks may be faster, cheaper, or have a wider reach. Moreover, many high-bandwidth connections route traffic based on complex contractual arrangements, which take into account factors such as cost, the type of traffic, or the balance between inbound and outbound traffic. Networks that are strategically well-connected and have high bandwidth are likely to be used for transit by packets coming from other, less-well-connected networks. These more strategically connected networks, which often link large metropolitan areas, are collectively referred to as the internet "backbone." The overwhelming majority of backbone links are fiber-optic cables, because fiber-optic connections have high bandwidth and can distribute data over long distances.

46. The internet backbone includes the approximately 49 international submarine cables that carry internet communications into and out of the United States and that land at approximately 43 different points within the country. The vast majority of international traffic into and out of the United States traverses this limited number of submarine cables.

Upstream Surveillance

47. The NSA conducts Upstream surveillance by connecting surveillance devices to multiple major internet cables, switches, and routers on the internet backbone inside the United

States. These access points are controlled by the country's largest telecommunications providers, including Verizon Communications, Inc. and AT&T, Inc. In some or all instances, aspects of Upstream surveillance may be conducted by the telecommunications providers on the government's behalf.

48. Upstream surveillance is intended to enable the comprehensive monitoring of international internet traffic. With the assistance of telecommunications providers, the NSA intercepts a wide variety of internet communications, including emails, instant messages, webpages, voice calls, and video chats. It copies and reviews substantially all international emails and other "text-based" communications—*i.e.*, those whose content includes searchable text.

49. More specifically, Upstream surveillance encompasses the following processes, some of which are implemented by telecommunications providers acting at the NSA's direction:

- **Copying.** Using surveillance devices installed at key access points along the internet backbone, the NSA makes a copy of substantially all international text-based communications—and many domestic ones—flowing across certain high-capacity cables, switches, and routers. The copied traffic includes email, internet-messaging communications, web-browsing content, and search-engine queries.

- **Filtering.** The NSA attempts to filter out and discard some wholly domestic communications from the stream of internet data, using IP filters for instance, while preserving international communications. The NSA's filtering out of domestic communications is incomplete, however, for multiple reasons. Among them, the NSA does not eliminate bundles of domestic and international communications that transit the internet backbone together. Nor does it eliminate domestic communications that happen to be routed abroad.

- **Content Review.** The NSA reviews the copied communications—including their full content—for instances of its search terms. The search terms, called "selectors," include email addresses, phone numbers, IP addresses, and other identifiers that NSA analysts believe to be associated with foreign intelligence targets. Again, the NSA's targets are not limited to suspected foreign agents and terrorists, nor are its selectors limited to individual email addresses. The NSA may monitor or "task" selectors used by large

groups of people who are not suspected of any wrongdoing—such as the IP addresses of computer servers used by hundreds of different people.

- **Retention and Use.** The NSA retains all communications that contain selectors associated with its targets, as well as those that happened to be bundled with them in transit. As discussed further below, NSA analysts may read, query, data-mine, and analyze these communications with few restrictions, and they may share the results of those efforts with the FBI, including in aid of criminal investigations.

50. One aspect of the processes outlined above bears emphasis: Upstream surveillance is not limited to communications sent or received by the NSA's targets. Rather, it involves the surveillance of essentially *everyone's* communications. The NSA systematically examines the full content of substantially all international text-based communications (and many domestic ones) for references to its search terms. In other words, the NSA copies and reviews the communications of millions of innocent people to determine whether they are discussing or reading anything containing the NSA's search terms. The NSA's practice of reviewing the *content* of communications for selectors is sometimes called "about" surveillance. This is because its purpose is to identify not just communications that are to or from the NSA's targets but also those that are merely "about" its targets. This is the digital analogue of having a government agent open every piece of mail that comes through the post to determine whether it mentions a particular word or phrase. Most pieces of mail—or email—will contain nothing of interest, but the government must still look through each one to find out. Although it could do so, the government makes no meaningful effort to avoid the interception of communications that are merely "about" its targets; nor does it later purge those communications.

51. Prior to the summer of 2013, the government had not publicly disclosed the fact that, under the FAA, it routinely reviews communications that are neither to nor from its targets. As the Privacy and Civil Liberties Oversight Board observed, "The fact that the

government engages in such collection is not readily apparent from the face of the statute, nor was collection of information 'about' a target addressed in the public debate preceding the enactment of FISA or the subsequent enactment of the FISA Amendments Act."

Targeting and Minimization Procedures

52. As indicated above, the FAA requires the government to adopt targeting and minimization procedures that govern who may be targeted for surveillance by executive-branch employees and how communications are to be handled once intercepted. These procedures are extremely permissive, and to the extent they impose limitations, those restrictions are riddled with exceptions.

53. Nothing in the targeting procedures meaningfully constrains the government's selection of foreign targets. Nor do the targeting procedures require the government to take measures to avoid intercepting U.S. persons' international communications. The targeting procedures expressly contemplate "about" surveillance, and thus the interception and review of communications between non-targets.

54. The minimization procedures are equally feeble. They impose no affirmative obligation on the NSA to promptly identify and purge U.S. persons' communications once they have been obtained. Rather, they allow the NSA to retain communications gathered via Upstream surveillance for as long as three years by default. It can retain those communications indefinitely if the communications are encrypted; if they are found to contain foreign intelligence information (again, defined broadly); or if they appear to be evidence of a crime. Indeed, the NSA may even retain and share wholly domestic communications obtained through the accidental targeting of U.S. persons if the NSA determines that the communications contain "significant foreign intelligence information" or evidence of a crime. The minimization

procedures also expressly contemplate that the NSA will intercept, retain, and disseminate attorney-client privileged communications. The minimization procedures bar the NSA from querying Upstream data using identifiers associated with specific U.S. persons, but they do not otherwise prohibit the NSA from conducting queries designed to reveal information to, from, or about U.S. persons.

The Surveillance of Plaintiffs

55. Plaintiffs are educational, legal, human rights, and media organizations. Their work requires them to engage in sensitive and sometimes privileged communications, both international and domestic, with journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses, among others.

56. By intercepting, copying, and reviewing substantially all international text-based communications—and many domestic communications as well—as they transit telecommunications networks inside the United States, the government is seizing and searching Plaintiffs' communications in violation of the FAA and the Constitution.

57. The conclusion that the government is seizing and searching Plaintiffs' communications is well-founded for at least four reasons.

58. First, the sheer volume of Plaintiffs' communications makes it virtually certain that the NSA has intercepted, copied, and reviewed at least some of their communications. In the course of a year, Plaintiffs collectively engage in more than one trillion international internet communications. As explained further below, Upstream surveillance could achieve the government's stated goals only if it entailed the copying and review of a large percentage of international text-based traffic. However, even if one assumes a 0.00000001% chance—one one-hundred millionth of one percent—of the NSA copying and reviewing any particular

communication, the odds of the government copying and reviewing at least one of the Plaintiffs' communications in a one-year period would be greater than 99.9999999999%.

59. In reality, this calculation understates the likelihood that the NSA has intercepted, copied, and reviewed Plaintiffs' communications, because large swaths of internet traffic that are not amenable to the text-based searches conducted in the course of Upstream surveillance and are likely of no foreign-intelligence interest to the government. By some estimates, for example, two-thirds of internet traffic consists of video traffic. The NSA could readily configure its surveillance equipment to ignore that traffic, or at least the significant portions of it (e.g., Netflix traffic) that are almost certainly of no interest. Because of the substantial efficiency gains to be had, it is extremely likely that the government engages in this kind of filtering, allowing it to more comprehensively monitor text-searchable traffic like that of Plaintiffs.

60. Second, the geographic distribution of Plaintiffs' contacts and communications across the globe makes it virtually certain that the NSA has intercepted, copied, and reviewed Plaintiffs' communications. As noted above, the internet backbone includes the approximately 49 international submarine cables carrying the vast majority of internet traffic into and out of the United States. It also includes the limited number of high-capacity terrestrial cables that carry traffic between major metropolitan areas within the United States, or between the United States and Canada or Mexico. The junctions where these backbone cables meet are in essence "chokepoints"—because almost all international internet traffic (as well as a significant share of domestic traffic) flows through one or more of them. Prime examples are the points where international submarine cables come ashore. The government has acknowledged using

Upstream surveillance to monitor communications at "international Internet link[s]" on the internet backbone.

61. Given the relatively small number of international chokepoints, the immense volume of Plaintiffs' communications, and the fact that Plaintiffs communicate with individuals in virtually every country on earth, Plaintiffs' communications almost certainly traverse every international backbone link connecting the United States with the rest of the world.

62. Third, and relatedly, in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link. That is because, as a technical matter, the government cannot know beforehand which communications will contain selectors associated with its targets, and therefore it must copy and review all international text-based communications transiting that circuit in order to identify those of interest. As the Privacy and Civil Liberties Oversight Board explained with respect to Upstream surveillance, "Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them." Because backbone cables carry vast amounts of internet traffic, the number of communications whose contents will be copied and reviewed will be enormous, regardless of how many the government ultimately retains.

63. There is an even more basic reason that, in conducting Upstream surveillance, the government must be monitoring all the international text-based communications that travel across a given link. To search the contents of any text-based communication for instances of the NSA's "selectors" as that communication traverses a particular backbone link, the

government must first copy and reassemble all of the packets that make up that communication. Those packets travel independently of one another, intermingled with packets of other communications in the stream of data. Where the government seeks to identify communications to, from, or about its many targets, as it does using Upstream surveillance, the packets of interest cannot be segregated from other, unrelated packets in advance. Rather, in order to reliably intercept the communications it seeks, the government must first copy *all* such packets traversing a given backbone link, so that it can reassemble and review the transiting communications in the way it has described.

64. In short, for every backbone link that the NSA monitors using Upstream surveillance, the monitoring must be comprehensive in order for the government to accomplish its stated goals. Accordingly, even if the NSA conducts Upstream surveillance on only a single internet backbone link, it must be intercepting, copying, and reviewing at least those communications of Plaintiffs traversing that link. In fact, however, the NSA has confirmed that it conducts Upstream surveillance at more than one point along the internet backbone, through the compelled assistance of multiple major telecommunications companies.

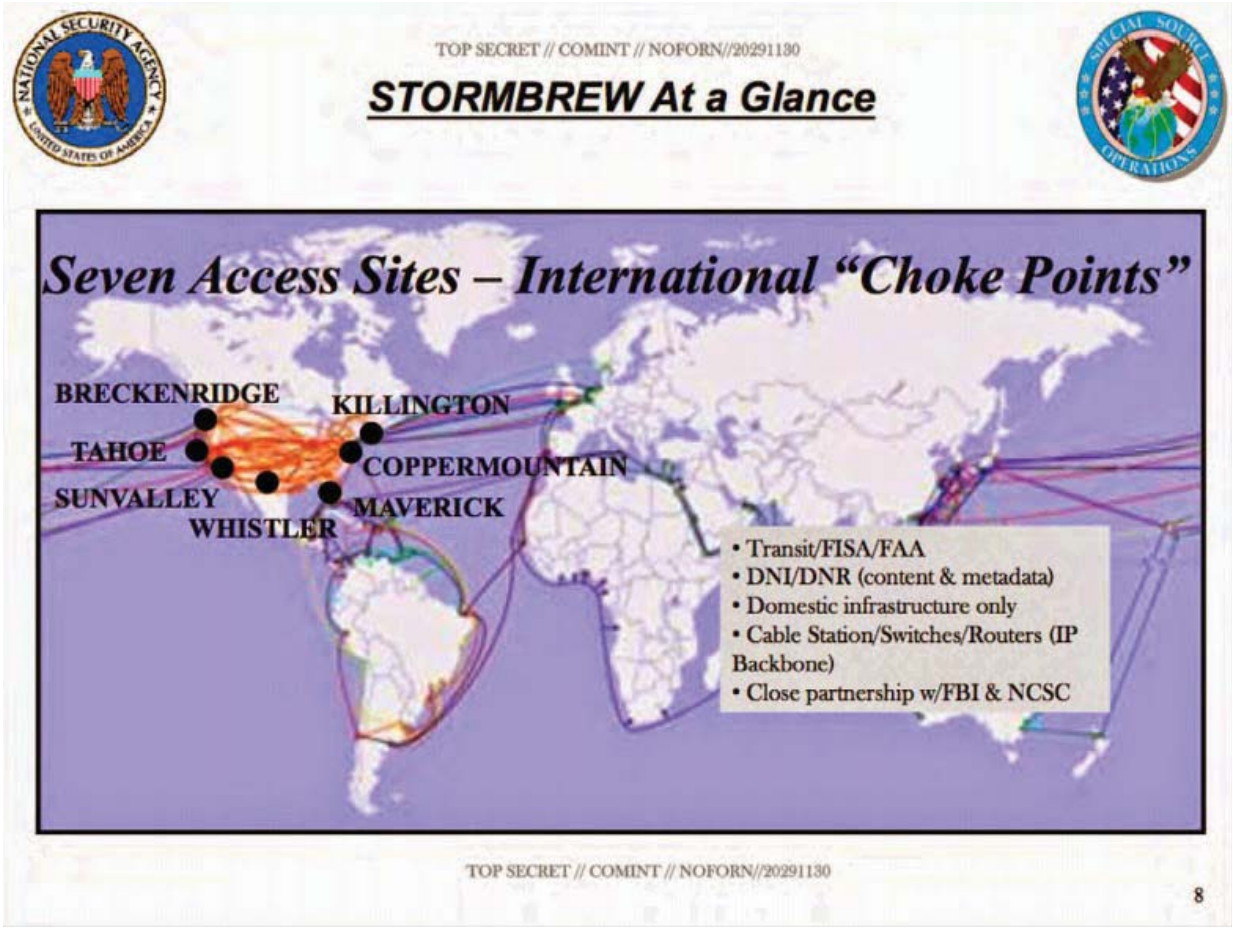
65. Fourth, given the way the government has described Upstream surveillance, it has a strong incentive to intercept communications at as many backbone chokepoints as possible. The government's descriptions of Upstream surveillance make clear that the government is interested in obtaining, with a high degree of confidence, all international communications to, from, or about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." And it has said about Upstream

surveillance more generally that its "success . . . depends on collection devices that can reliably acquire data packets associated with the proper communications."

66. If the government's aim is to "comprehensively" and "reliably" obtain communications to, from, and about targets scattered around the world, it must conduct Upstream surveillance at many different backbone chokepoints. That is especially true because the communications of individual targets may take multiple paths when entering or leaving the United States. When two people communicate in real-time, the communications they exchange frequently take different routes across the internet backbone, even though the end-points are the same. In other words, in the course of a single exchange, the communications *from* a target frequently follow a different path than those *to* the target. Relatedly, a target's location may vary over time, as do the network conditions that determine a given communication's path from origin to destination. As a result, a target's communications may traverse one backbone cable or chokepoint at one moment, but a different one later. In fact, as the Privacy and Civil Liberties Oversight Board observed, even a single email "can be broken up into a number of data packets that take different routes to their common destination." Because of these variables, Upstream surveillance would be comprehensive only if it were implemented at a number of backbone chokepoints.

67. For the four reasons stated above, it is a virtual certainty that the NSA is intercepting, copying, and reviewing Plaintiffs' communications.

68. This conclusion is corroborated by government documents that have been published in the press. For example, one NSA slide illustrates the Upstream surveillance facilitated by just a single provider (referred to as "STORMBREW") at seven major international chokepoints in the United States:



69. Similarly, another NSA document states that, in support of FAA surveillance, the "NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." In fact, in describing the scale and operation of Upstream surveillance, *The New York Times* has reported, based on interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border."

70. The government's interception, copying, and review of Plaintiffs' communications while in transit is a violation of Plaintiffs' reasonable expectation of privacy in

those communications. It is also a violation of Plaintiffs' right to control those communications and the information they reveal and contain.

71. Furthermore, because of the nature of their communications, and the location and identities of the individuals and groups with whom and about whom they communicate, there is a substantial likelihood that Plaintiffs' communications intercepted by the NSA through Upstream surveillance are retained, read, and disseminated.

72. The retention, reading, and dissemination of Plaintiffs' communications is a further, discrete violation of Plaintiffs' reasonable expectation of privacy in those communications. It is also a further, discrete violation of Plaintiffs' right to control those communications and the information they reveal and contain.

73. Plaintiffs, in connection with constitutionally protected activities, communicate with people whom the government is likely to target when conducting Upstream surveillance, including foreign government officials, journalists, experts, human rights defenders, victims of human rights abuses, and individuals believed to have information relevant to counterterrorism efforts.

74. A significant amount of the information that Plaintiffs exchange over the internet is "foreign intelligence information" within the meaning of the FAA.

75. Because of ongoing government surveillance, including Upstream surveillance, Plaintiffs have had to take burdensome and sometimes costly measures to minimize the chance that the confidentiality of their sensitive information will be compromised. Plaintiffs have variously had to develop new protocols for transmitting sensitive information, to travel long distances to collect information that could otherwise have been shared electronically, and in some circumstances to forgo particularly sensitive communications altogether.

76. Because of ongoing government surveillance, including Upstream surveillance, Plaintiffs are not able to gather and relay information, represent their clients, and engage in domestic and international advocacy as they would in the absence of the surveillance. Upstream surveillance reduces the likelihood that clients, users, journalists, witnesses, experts, civil society organizations, foreign government officials, victims of human rights abuses, and other individuals will share sensitive information with Plaintiffs.

77. Upstream surveillance is inhibiting the constitutionally protected communications and activities of Plaintiffs and others not before the Court.

Wikimedia Foundation

78. Wikimedia is a non-profit organization dedicated to encouraging the growth, development, and distribution of free, multilingual, educational content. In this effort, it develops and maintains "wiki"-based projects, and provides the full contents of those projects to individuals around the world free of charge. At present, Wikimedia operates twelve free-knowledge projects ("Projects") as well as other related websites and pages on the internet.

79. The best-known of Wikimedia's Projects is Wikipedia—a free internet encyclopedia that is one of the top ten most-visited websites in the world and one of the largest collections of shared knowledge in human history. In 2014, Wikipedia contained more than 33 million articles in over 275 languages, and Wikimedia sites received between approximately 412 and 495 million monthly visitors. Wikipedia's content is collaboratively researched and written by millions of volunteers, many of whom choose not to identify themselves, and is in most instances open to editing by anyone. Volunteers also use Wikipedia discussion forums and "discussion pages" to debate the editorial policies and decisions required for reliable and neutral content.

80. Other Projects include Wikimedia Commons, an online repository of free images, sound, and other media files; Wikinews, a collaborative journalism platform for volunteers to create and edit original news articles; and Wikibooks, a platform for the creation of free textbooks and annotated texts that anyone can edit consistent with the policies of the site.

81. Wikimedia encourages individuals around the world to contribute to the Projects by communicating information to Wikimedia. Wikimedia receives and maintains this information, and subsequently communicates it to the many other individuals who seek to access, engage with, and further add to Wikimedia's store of knowledge. The principal way in which Wikimedia communicates with its community—which, at its broadest level, consists of individuals who access or contribute to the body of knowledge comprising the twelve Projects—is via the internet.

82. Wikimedia provides the technical infrastructure for the Projects, much of which is hosted on Wikimedia's servers in Virginia, Texas, and California. In addition, Wikimedia develops software and provides tools for others to develop software platforms; develops mobile phone applications and enters into partnerships; administers grants to support activity that benefits the Wikimedia user community and the Wikimedia movement; provides administrative support to grantees; works with community members to organize conferences and community-outreach events globally; and engages in advocacy on issues that affect the Wikimedia community.

83. Wikimedia maintains an active and close relationship with the volunteers, contributors, and many other users who comprise the Wikimedia community. Wikimedia exists for this community and depends upon it: the user community plays a vital role in many of

Wikimedia's functions, including the creation of Wikimedia content, the development and enforcement of Wikimedia policies, the donation of funds that help Wikimedia thrive, and the governance of the organization as a whole. In short, Wikimedia operates interdependently with its user community in pursuit of a shared set of free-knowledge values.

84. Wikimedia's corporate structure and decision-making reflect this interdependence. In accordance with Wikimedia's bylaws, at least half of Wikimedia's Board of Trustees is selected by Wikimedia community members. That Board relies, in turn, on several user-staffed committees to oversee Board elections, consider grant applications, and recommend new Wikimedia chapters or community organizations. More generally, Wikimedia makes core organizational decisions after soliciting the input and preferences of its users on topics including its public-policy positions, the creation of new features and Projects, corporate strategy, and budgetary matters. For instance, Wikimedia staff frequently engage in "Community Consultations," in which community members can offer their views on these and other matters directly.

85. Wikimedia's community of volunteers, contributors, and readers consists of individuals in virtually every country on earth. Among many others, the Wikimedia community includes U.S. persons who are located abroad and who engage in international communications with Wikimedia.

86. Upstream surveillance implicates at least three categories of Wikimedia communications: (i) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other; (ii) Wikimedia's internal "log" communications, which help it to

monitor, study, and improve its community members' use of the Projects; and (iii) communications by Wikimedia staff.

87. As the operator of one of the most-visited websites in the world, Wikimedia engages in an extraordinarily high volume of internet communications. From April 1, 2014 to March 31, 2015, Wikimedia websites received over 255 billion "page views." Over the lifespan of the Wikimedia Projects, Wikimedia's users have edited its pages more than two billion times. Each of these activities involves internet communications between Wikimedia and its users—the majority of whom are located abroad.

88. Indeed, Wikimedia engages in more than one trillion international communications each year, with individuals who are located in virtually every country on earth. For a user to view, search, log in, edit, or contribute to a Wikimedia Project webpage, the user's device must send at least one HTTP or HTTPS "request" to a Wikimedia server. "HTTP" and "HTTPS" are common protocols for transmitting data via the internet, including the content of many webpages. The number of requests required for a user to access a particular webpage depends on the number of graphics, videos, and other specialized components featured on the page. After receiving such a user request, the Wikimedia server transmits an HTTP or HTTPS "response" to the user's device, where the content of the requested webpage component is rendered and displayed to the user. In May 2015, Wikimedia's U.S.-based servers received more than 88 billion HTTP or HTTPS requests from outside the United States. At this rate, Wikimedia receives more than one trillion HTTP or HTTPS requests annually, and transmits more than one trillion HTTP or HTTPS responses back to those Wikimedia users abroad.

89. Wikimedia's HTTP and HTTPS communications are essential to its organizational mission, as is its ability to control and maintain the privacy of these communications. The communications reveal and contain some of the most sensitive information that Wikimedia possesses: which specific webpages each particular person is editing or visiting. In other words, they reveal who is reading—or writing—what.

90. For example, among other private information, HTTP and HTTPS requests reveal or contain the user's IP address; the URL of the webpage sought by the user, which often conveys information about the content of the requested page; and the "user agent," which may identify the manufacturer, model, version, and other information about the user's device. Many requests also contain other types of private information, such as a user's log-in credentials; the referrer, which reflects information about the previous webpage the user visited; the search terms a user entered to query Wikimedia's webpages; "cookies," which include information that can be used to link a user to his or her prior Wikimedia requests and prior approximate geolocation; a user's non-public "draft" contributions to Wikimedia; or a user's private questions, comments, or complaints, submitted via Wikimedia's online feedback platform.

91. In much the same way, Wikimedia's HTTP and HTTPS responses may reveal or contain, among other private information, the user's IP address; the content of the requested webpage component; the URL of the webpage the user should be redirected to; "cookies," which include information used to link a user to subsequent Wikimedia requests and his or her approximate geolocation; search terms; a user's username; a user's non-public "draft" contributions; and a user's private questions, comments, or complaints.

92. In furtherance of its mission, Wikimedia also frequently engages in communications that permit its users to interact with one another more directly. For example, a

registered user of Wikimedia may send an email via Wikimedia to another registered user, so long as both have enabled email communications on their Wikimedia accounts. Similarly, Wikimedia engages in communications that allow users to interact in small or limited groups—including over wikis that only certain users, such as user-community leaders, have access to, and mailing lists with restricted membership. Some of these communications are transmitted via HTTP or HTTPS; others rely on different protocols. All of these interactions involve communications between Wikimedia and its community members.

93. The second category of Wikimedia communications are its internal, proprietary "log" communications, which help it to monitor, study, and improve the Projects. In particular, every time Wikimedia receives an HTTP or HTTPS request from a person accessing a Project webpage, it creates a corresponding log entry. Among other private information, logs contain the user's IP address; the URL of the webpage sought by the user; the time the request was received by Wikimedia's server; and the "user agent," which may identify the manufacturer, model, version, and other information about the user's device. Depending on the location of the user and the routing of her request, the log may be generated by Wikimedia's servers abroad, which in turn send the log to Wikimedia in the United States. In May 2015, Wikimedia transmitted more than 140 billion logs from its servers abroad to its servers in the United States. The organization relies on its logs for a variety of analytical projects, which are designed to improve Wikimedia's operations and the experience of those using the Projects.

94. Wikimedia's communications with its community members—as well as its internal logs—link each user's page views, searches, and contributions with his or her IP address, as well as with other user-specific information. As a rule, Wikimedia maintains as private the IP addresses associated with its community members and their individual

interactions with the Projects, except in those instances where an individual editor reveals his or her IP address publicly (i.e., is not logged in as a registered user). IP addresses, like telephone numbers, are often personally identifying, especially in conjunction with other information about a given communication or internet user. It is generally trivial to link a particular IP address with a particular person—thereby revealing his or her online activities—in part because internet service providers routinely maintain records of the IP addresses assigned to their network subscribers over time.

95. Because of the information they contain, Wikimedia's communications with its community members, as well as its internal communications related to the study and improvement of the Projects, are often sensitive and private. These communications reveal a detailed picture of the everyday concerns and reading habits of Wikimedia's users, and often constitute a record of their political, religious, sexual, medical, and expressive interests.

96. Seizing and searching Wikimedia's communications is akin to seizing and searching the patron records of the largest library in the world—except that Wikimedia's communications provide a more comprehensive and detailed picture of its users' interests than any previous set of library records ever could have offered.

97. Upstream surveillance permits the government to observe—continuously—which of Wikimedia's millions of webpages are being read or edited at any given moment, and by whom. Moreover, it allows the government to review those communications for any reference to its tens of thousands of search terms, and to retain a copy of any communication that is of interest.

98. As an organization, Wikimedia has an acute privacy interest in its communications—one on par with that of users themselves. That is because Wikimedia's

mission and existence depend on its ability to ensure that readers and editors can explore and contribute to the Projects privately when they choose to do so. Wikimedia's communications reveal who has contributed to the Projects or visited them in search of information—and, just as importantly, exactly *what* information Wikimedia has exchanged with any individual user. With the partial exception of editors who publicly disclose their IP addresses, these exchanges are not public; they are private interactions between Wikimedia and its community members. If it were otherwise, Wikimedia would have immense difficulty both gathering content and sharing information as widely as possible. This privacy is necessary to foster trust with community members and to encourage the growth, development, and distribution of free educational content.

99. Wikimedia's communications also reveal private information about its operations, including details about its technical infrastructure, its data flows, and its member community writ large.

100. Wikimedia takes steps to protect the privacy of its communications and the confidentiality of the information it thereby receives. For instance, because of the sensitivity of Wikimedia's communications with its community members, Wikimedia seeks to collect and retain as little information about those exchanges as possible. Where it does collect such information, Wikimedia strives to keep it for only a limited amount of time, consistent with the maintenance, understanding, and improvement of the Projects and with Wikimedia's legal obligations. Still, Wikimedia possesses a large volume of sensitive information about its interactions with its community members, and it transmits a large volume of sensitive information about those interactions every day.

101. Wikimedia defends the privacy of its communications in other ways, including through both technical measures and legal action. Wikimedia undertakes costly and burdensome measures to ensure the security of its communications and the data it retains as a result. Wikimedia also assures its community via policies, public statements, and guidelines that it will reject third-party requests for non-public user information unless it is legally required to disclose that information. In keeping with these assurances, Wikimedia resists third-party demands for information that are overly broad, unclear, or irrelevant; notifies users individually of information requests when legally permitted; and provides legal defense funds for certain community members who are subject to lawsuits or demands for non-public information as a result of their participation in the Projects.

102. Wikimedia also engages in a third category of sensitive communications. Certain members of Wikimedia's staff routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad in carrying out Wikimedia's work.

103. Wikimedia's communications—with its community members, its internal communications, and its staff communications—are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of Wikimedia, its staff, and its users, and it violates their right to control those communications and the information they contain.

104. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Wikimedia's international communications because Wikimedia is communicating with or about persons the government has targeted for Upstream surveillance. Wikimedia's international contacts include foreign telecommunications companies, foreign government

officials, political and business leaders, universities, Wikimedia users and their legal counsel, Wikimedia trustees and international contractors, Wikimedia's international outside legal counsel, project partners, grantees, and volunteers—some of whom are likely targets. Wikimedia's communications with these contacts sometimes concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Wikimedia communicates both with and about these likely targets. Wikimedia's international communications contain, among other things, information about its foreign contacts, including the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Wikimedia's work.

105. Moreover, more than one trillion of Wikimedia's international communications each year—its HTTP and HTTPS transmissions as well as its internal logs of user activity—contain details such as website addresses and IP addresses. Whenever a Wikimedia user abroad edits or contributes to a Project webpage that happens to reference one of the NSA's selectors, Wikimedia engages in an international communication containing that selector. The same is often true when a Wikimedia user abroad simply reads such a Project webpage. Some of these communications are likely retained, read, and disseminated in the course of Upstream surveillance.

106. Because Wikipedia is a comprehensive encyclopedic resource, it includes entries related to virtually any foreign organization or company the U.S. government might target for Upstream surveillance. Many of these entries contain website addresses and domain names associated with those likely targets. Notably, website addresses or domain names associated with organizations on the U.S. State Department's Foreign Terrorist Organization list appear over 700 times on Project webpages—including those describing organizations, like

Uzbekistan's Islamic Jihad Union, whose communications the U.S. government has targeted using FAA surveillance.

107. The NSA has expressed interest in surveilling Wikimedia's communications. An NSA slide disclosed by the media asks, "Why are we interested in HTTP?" It then answers its own question: "Because nearly everything a typical user does on the Internet uses HTTP." This statement is surrounded by the logos of major internet companies and websites, including Facebook, Yahoo, Twitter, CNN.com, and Wikipedia. The slide indicates that, by monitoring HTTP communications, the NSA can observe "nearly everything a typical user does" online—including individuals' online reading habits and other internet activities. This information is queried and reviewed by analysts using a search tool that allows NSA analysts to examine data intercepted pursuant to the FAA and other authorities.

108. Upstream surveillance undermines Wikimedia's ability to conduct its work. Wikimedia depends on its ability to ensure anonymity for individuals abroad who view, edit, or otherwise use Wikimedia Projects and related webpages. The ability to read, research, and write anonymously is essential to the freedoms of expression and inquiry. In addition, Wikimedia's staff depend on the confidentiality of their communications, including in some cases their ability to ensure that their contacts' identities will not be revealed. Because of these twin needs for anonymity and confidentiality, Upstream surveillance harms the ability of Wikimedia's staff to engage in communications essential to their work and compromises Wikimedia's organizational mission by making online access to knowledge a vehicle for U.S. government monitoring.

109. Due in part to NSA surveillance, including Upstream surveillance, Wikimedia has undertaken burdensome and costly measures to protect its communications, including adopting more secure methods of electronic communication, and in some instances self-censoring communications or forgoing electronic communications altogether. These measures divert Wikimedia's time and monetary resources as a non-profit entity from other important organizational work.

110. Despite these precautions, Wikimedia believes that Upstream surveillance has resulted and will result in some foreign readers, editors, contributors, and volunteers being less willing to read, contribute to, or otherwise engage with Wikimedia's Projects. For instance, some Wikimedia users have expressed reluctance to continue participating in the Wikimedia movement because of U.S. government surveillance, including FAA surveillance. The loss of these foreign users is a direct detriment to Wikimedia, its ability to receive information and associate with its community members, and its organizational goal of increasing global access

to knowledge. It also harms Wikimedia's domestic users, who do not have access to information and opinions that Wikipedia's foreign contributors would otherwise have provided. Similarly, Wikimedia believes that Upstream surveillance reduces the likelihood that Wikimedia's foreign volunteers, grantees, and other contacts will communicate with staff members, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

111. Because Wikimedia's community members are so numerous, because they are dispersed across the globe, and because millions of them choose to interact with Wikimedia anonymously, their rights are likely to be impaired if Wikimedia is unable to assert claims on their behalf. That is especially so because Wikimedia is uniquely capable of presenting the aggregate effects that Upstream surveillance has on community members' ability to contribute to the Projects and to receive information from others.

National Association of Criminal Defense Lawyers

112. The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C. NACDL's mission is to foster the integrity, independence, and expertise of the criminal defense profession, and to promote the proper and fair administration of justice. NACDL has approximately 9,200 members as well as 90 local, state, and international affiliate organizations with approximately 40,000 members. NACDL's interest in challenging the lawfulness of Upstream surveillance is germane to the organization's mission and purpose, and to its relationship with its members. As explained below, because unlawful U.S. government surveillance profoundly affects the ability of

criminal defense attorneys to ensure that accused persons receive effective counsel, such surveillance interferes with the proper and fair administration of justice.

113. As defense attorneys, NACDL's members engage in international and domestic internet communications that are essential to the effective representation of their clients. Among other things, NACDL's members routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad as part of their representations.

114. The communications of NACDL's members are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of members' communications and it violates their right to control their communications and the information they contain.

115. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates international communications of NACDL's members because they are communicating with or about persons the government has targeted for Upstream surveillance. In the course of their representations, NACDL members communicate internationally with clients, clients' families, witnesses, journalists, human rights organizations, experts, investigators, and foreign government officials, some of whom are likely targets. Their communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." NACDL members communicate both with and about these likely targets. Members' international communications contain, among other things, details about their foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to their work.

116. One group of NACDL members is especially likely to have their communications retained, read, and disseminated in the course of Upstream surveillance: defense attorneys who represent individuals in criminal prosecutions in which the government has acknowledged its use FAA surveillance. In these cases, the government's prosecution of the defendant is based on evidence obtained from an FAA target. As a result, defense attorneys are especially likely to engage in communications to, from, or about FAA targets in the course of investigating the government's allegations, contacting witnesses, and collecting their own evidence. Indeed, in several of these cases, the targeted selector—*e.g.*, the targeted email address—has been identified in press reports or may be ascertained from congressional testimony and court filings. NACDL defense attorneys who communicate internationally with or about that targeted selector will have their communications retained by the government, much as their clients' communications were warrantlessly intercepted and retained.

117. NACDL members have an ethical obligation to protect the confidentiality of their clients' information, including information covered by the attorney-client privilege.

118. Upstream surveillance compromises NACDL members' ability to comply with their ethical obligations and undermines their effective representation of their clients. Members' defense work depends on the confidentiality of their communications, including their ability to assure contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, NACDL's members have undertaken burdensome and costly measures to protect their communications, including adopting more secure methods of electronic communication, traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, NACDL believes that

Upstream surveillance reduces the likelihood that potential sources, witnesses, experts, and foreign government officials will share sensitive information with NACDL's members, because those contacts fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

NACDL Member Joshua L. Dratel

119. Joshua L. Dratel is a nationally recognized criminal defense lawyer in New York City who has been a member of NACDL since 1985. He is Chair of NACDL's National Security Committee, co-Chair of NACDL's Select Committee on Military Tribunals, and Co-Chair of its Amicus Curiae Committee. From 2003 to 2009, he served as a member of the Board of Directors of NACDL. He is also co-editor of *The Torture Papers: The Legal Road to Abu Ghraib* (Cambridge University Press 2005).

120. Mr. Dratel's litigation experience encompasses all aspects of criminal defense, and among other clients, he represents individuals accused of internet- and terrorism-related crimes. For example, he defended Wadith El Hage in *United States v. Usama Bin Laden*, the prosecution resulting from the 1998 bombings of the U.S. embassies in Kenya and Tanzania. Mr. Dratel also represented David Hicks—who was detained at Guantánamo Bay for six years—in U.S. military commission proceedings. The U.S. Court of Military Commission Review recently overturned Mr. Hicks's conviction for material support for terrorism. Mr. Dratel's current clients include Baasaly Moalin, who is appealing from a conviction of charges of material support for terrorism.

121. Mr. Dratel's law practice also includes a client who has received notice of FAA surveillance, and he previously represented a client in another case where officials have told

Congress that the government used FAA surveillance in the course of its investigation. He has defended other individuals in prosecutions where there is reason to believe the government relied on such surveillance.

122. In connection with his defense work and confidential consultations with defense attorneys in other national security-related cases, Mr. Dratel routinely engages in both domestic and international communications via the internet. Many of the individuals with whom he exchanges information are located abroad, and are neither U.S. citizens nor permanent residents. Their communications occur via email, instant messenger, and text messaging.

123. The vast majority of Mr. Dratel's international communications as a defense attorney are sensitive, and many of them are privileged or otherwise protected from disclosure by the attorney work-product doctrine.

124. Mr. Dratel's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of his communications and it violates his right to control his communications and the information they contain.

125. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Mr. Dratel's international communications because he is communicating with persons the government has targeted for Upstream surveillance. In the course of his representations, Mr. Dratel communicates internationally with clients, clients' families, lawyers, witnesses, journalists, human rights organizations, experts, investigators, and foreign government officials, some of whom are likely targets. Most notably, his international contacts include individuals the U.S. government has targeted for prosecution for terrorism-related crimes, as well as their families, friends, and associates, including their attorneys overseas. For example, Mr. Dratel communicates via the internet with his former client, Mr. Hicks, who lives

in Australia following his release from Guantánamo Bay. In addition, Mr. Dratel's communications with his international contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Mr. Dratel also communicates with likely FAA targets when he visits websites hosted overseas on the internet. This internet browsing involves communications with selectors—such as domain names and IP addresses—that the NSA has likely targeted for FAA surveillance. In his representation of defendants charged with terrorism-related crimes, it is often necessary for him to review websites maintained by terrorist organizations abroad, so that he can understand the facts related to certain investigations and prosecutions.

126. Similarly, there is a substantial likelihood that the NSA retains, reads, and disseminates Mr. Dratel's international communications because he is communicating *about* persons the government has targeted for Upstream surveillance. Mr. Dratel's international communications contain, among other things, details about his foreign contacts and other important sources of information—details such as the email addresses, phone numbers, social media identities, and website addresses of foreign individuals and organizations relevant to his work.

127. The fact that Mr. Dratel's clients have been subject to FAA surveillance themselves, or involved in investigations where others were subject to such surveillance, makes the NSA's retention and dissemination of Mr. Dratel's own communications especially likely. In representing these clients, Mr. Dratel is almost certain to engage in communications to, from, or about FAA targets in the course of investigating the government's allegations, contacting witnesses, and collecting evidence abroad via the internet. When Mr. Dratel

communicates with or about persons and selectors targeted under the FAA, he is subject to FAA surveillance just like his clients.

128. Due in part to U.S. government surveillance, including Upstream surveillance, Mr. Dratel has had to undertake burdensome and costly measures to protect his international communications, and in certain instances has forgone those communications altogether. For example, Mr. Dratel has had to and will have to travel abroad to gather information in-person that he would otherwise have gathered by electronic communication. Such travel is time-consuming and costly. He has also paid for and will have to pay for investigators abroad to travel to the United States to meet with him in-person to discuss their cases. In addition, Mr. Dratel routinely relies on time-consuming security measures, such as Pidgin Encryption and PGP, to encrypt his domestic and international instant messages and emails, in an effort to protect especially sensitive privileged communications and work product. Mr. Dratel also routinely censors his own speech (and asks his international contacts to do the same) in electronic communications. These precautions and security measures are not voluntary; they are the result of Upstream surveillance and the rules of professional responsibility that apply to Mr. Dratel as an attorney.

129. As a general matter, Upstream surveillance compromises Mr. Dratel's ability to communicate with his clients overseas and to gather information relevant and necessary to his work. This surveillance makes it difficult, expensive, and sometimes impossible to obtain information from individuals outside of the United States. In some instances, the increased awareness of U.S. government surveillance has resulted and will result in clients, lawyers, and potential witnesses limiting the information that they share with Mr. Dratel and that he shares with them. Indeed, some witnesses abroad have not and will not communicate with Mr. Dratel

at all electronically, because they believe that by sharing information with him, they are also sharing information with the U.S. government. At times, Mr. Dratel must forgo these communications altogether. The cost of traveling to certain remote areas of the globe to interview a potential witness in-person can be too high to justify the travel, and some regions are simply too dangerous or inaccessible to permit in-person visits.

Human Rights Watch

130. HRW is a non-profit, non-governmental human rights organization based in New York City. It employs approximately 400 staff members located across offices around the world. Formed in 1978, HRW's mission is to defend the rights of people worldwide. HRW conducts fact-finding investigations into human rights abuses by governments and non-state actors in all regions of the world.

131. HRW engages in international and domestic internet communications that are essential to its mission. Among other things, HRW's U.S.-based staff routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out HRW's research, reporting, and advocacy work.

132. HRW's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of HRW's communications and it violates HRW's right to control those communications and the information they contain.

133. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates HRW's international communications because HRW is communicating with or about persons the government has targeted for Upstream surveillance. HRW's international contacts include foreign government officials, humanitarian agencies, think tanks, military officials, human rights defenders, politicians, dissidents, victims of human rights abuses,

perpetrators of human rights abuses, religious groups, media, and scholars, some of whom are likely targets. HRW's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." HRW communicates both with and about these likely targets. HRW's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to HRW's work.

134. Upstream surveillance undermines HRW's ability to conduct its work. HRW's research, reporting, and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, HRW has undertaken burdensome and costly measures to secure and protect its communications, including adopting more secure methods of electronic communication, traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, HRW believes that Upstream surveillance reduces the likelihood that sources, witnesses, experts, foreign government officials, and victims of human rights abuses will share sensitive information with HRW's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

Amnesty International USA

135. AIUSA, headquartered in New York City, is one of Amnesty International's largest national sections, with hundreds of thousands of members and supporters. Through its

advocacy campaigns, AIUSA seeks to expose and stop human rights abuses in the United States and throughout the world.

136. AIUSA engages in international and domestic internet communications that are essential to its mission. Among other things, some of AIUSA's U.S.-based staff—as well as some AIUSA members who serve as volunteer specialists on particular countries and thematic issues—routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out AIUSA's reporting and advocacy work.

137. AIUSA's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of AIUSA's communications and it violates AIUSA's right to control those communications and the information they contain.

138. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates AIUSA's international communications because AIUSA is communicating with or about persons the government has targeted for Upstream surveillance. AIUSA's international contacts include Amnesty International researchers who are documenting and witnessing human rights violations in the field, human rights defenders, victims of violations and their families, eyewitnesses to violations, political dissidents, government officials, journalists, and lawyers, some of whom are likely targets. AIUSA's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." AIUSA communicates both with and about these likely targets. AIUSA's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to AIUSA's work.

139. Upstream surveillance undermines AIUSA's ability to conduct its work. AIUSA's reporting and advocacy depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, some AIUSA staff strive to communicate particularly sensitive matters in-person, and must sometimes avoid sensitive topics or forgo exchanging information about these matters altogether. Despite these precautions, AIUSA believes that Upstream surveillance reduces the likelihood that sources, witnesses, experts, foreign government officials, and victims of human rights abuses will share sensitive information with AIUSA's staff and members, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

PEN American Center

140. PEN is an association based in New York City of approximately 4,000 novelists, journalists, editors, poets, essayists, playwrights, publishers, translators, agents, and other professionals, and an even larger network of readers and supporters. It is the largest of the organizations within PEN International. For the last 90 years, PEN has worked to ensure that people all over the world are at liberty to create literature, to convey ideas freely, and to express their views unimpeded. One of PEN's core projects is to advocate on behalf of persecuted writers across the globe, so that they might be free to write and to express their ideas.

141. PEN engages in international and domestic internet communications that are essential to its mission. Among other things, PEN's U.S.-based staff routinely engage in

sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out PEN's research and advocacy work.

142. PEN's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of PEN's communications and it violates PEN's right to control those communications and the information they contain.

143. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates PEN's international communications because PEN is communicating with or about persons the government has targeted for Upstream surveillance. PEN's international contacts include writers whose work and experiences relate to political upheavals, human rights violations, freedom of the press, and government surveillance; those writers' families and legal representatives; human rights defenders; and other PEN partners in countries such as Syria, Cuba, China, Iran, and Ethiopia—some of whom are likely targets. PEN's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." PEN communicates both with and about these likely targets. PEN's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to PEN's work.

144. Upstream surveillance undermines PEN's ability to conduct its work. PEN's research and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, PEN staff have undertaken burdensome measures to secure and protect their

communications, including adopting more secure methods of electronic communication, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, PEN believes that Upstream surveillance reduces the likelihood that foreign writers and other contacts will share sensitive information with PEN's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

Global Fund for Women

145. GFW, based in San Francisco and New York City, is a grant-maker and a global advocate for women's human rights. GFW advances the movement for women's human rights by directing resources to and raising the voices of women worldwide. GFW invests in local, courageous women and women-led organizations, and creates digital advocacy campaigns on critical global issues for women and girls. Since its inception in 1986, GFW has awarded 9,921 grants totaling $120 million to 4,759 organizations in 175 countries.

146. GFW engages in international and domestic internet communications that are essential to its mission. Among other things, GFW's U.S.-based staff routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad in carrying out GFW's grant-making and advocacy work.

147. GFW's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of GFW's communications and it violates GFW's right to control those communications and the information they contain.

148. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates GFW's international communications because GFW is communicating with or

about persons the government has targeted for Upstream surveillance. GFW's international contacts include foreign banks, foreign government agencies, funders, attorneys, and grantee and partner organizations working in conflict zones or on politically sensitive issues abroad, some of whom are likely targets. GFW's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." GFW communicates both with and about these likely targets. GFW's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to GFW's work.

149. Upstream surveillance undermines GFW's ability to conduct its work. GFW's grant-making depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, GFW's staff must exercise extreme caution when engaging in certain international communications, and in some instances avoid sensitive topics or forgo communications altogether. Some of GFW's international contacts will communicate with the organization only by phone or Skype, rather than email, because they believe that email is a less secure means of communication. Other of GFW's international contacts will communicate via email, but only if staff avoid using certain words in their communications that may result in further government scrutiny. Despite these precautions, GFW believes that Upstream surveillance reduces the likelihood that current and prospective grantees will share sensitive information with GFW's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the

other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Nation Magazine

150. The Nation is America's oldest weekly magazine of opinion, news, and culture. The Nation is also a digital media company, reporting daily on politics, social issues, and the arts. Its journalists report on a wide range of issues relating to international affairs, including the wars in Iraq and Afghanistan, the Israel–Palestine conflict, protest activities and politics in China and elsewhere in East Asia, and civil wars and other conflicts in Africa and Latin America.

151. The Nation engages in international and domestic internet communications that are essential to its mission. Among other things, The Nation's staff and contributing writers routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out The Nation's research, reporting, and editing.

152. The Nation's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of The Nation's communications and it violates The Nation's right to control those communications and the information they contain.

153. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates The Nation's international communications because The Nation is communicating with or about persons the government has targeted for Upstream surveillance. The Nation's international contacts include foreign journalists in conflict zones, foreign government officials, political dissidents, human rights activists, and members of guerrilla and insurgency movements, some of whom are likely targets. The Nation's communications with these

contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." The Nation communicates both with and about these likely targets. The Nation's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to The Nation's work.

154. Upstream surveillance undermines The Nation's ability to conduct its work. The Nation's research and reporting depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, The Nation has undertaken burdensome and costly measures to protect its communications, including adopting more secure methods of electronic communication, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, The Nation believes that Upstream surveillance reduces the likelihood that foreign journalists and sources will share sensitive information with The Nation, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Rutherford Institute

155. The Rutherford Institute, founded in 1982 and based in Virginia, is a civil liberties organization committed to protecting the constitutional freedoms of Americans and the human rights of all people. Rutherford provides free legal services in defense of civil liberties

and educates the public about constitutional and human rights issues. It also advocates on behalf of individuals abroad whose rights are threatened by foreign governments.

156. Rutherford engages in international and domestic internet communications that are essential to its mission. Among other things, Rutherford's staff, who are based in the U.S., routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out Rutherford's advocacy, legal, and educational activities.

157. Rutherford's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of Rutherford's communications, and it violates Rutherford's right to control those communications and the information they contain.

158. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Rutherford's international communications because Rutherford is communicating with or about persons the government has targeted for Upstream surveillance. Rutherford's international contacts include human rights and civil liberties advocates, foreign government officials, and individuals whose rights are threatened by the U.S. or foreign governments, some of whom are likely targets. Rutherford's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Rutherford communicates both with and about these likely targets. Rutherford's international communications, among other things, contain details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Rutherford's work.

159. Upstream surveillance undermines Rutherford's ability to conduct its work. Rutherford's advocacy depends on its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, Rutherford in some instances avoids sensitive topics or forgoes communications altogether. Rutherford believes that Upstream surveillance reduces the likelihood that victims of human rights abuses, witnesses, foreign government officials, and other contacts will share sensitive information with Rutherford, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Washington Office on Latin America

160. WOLA is a non-profit, non-governmental organization based in Washington D.C. WOLA works to advance human rights and social justice in the Americas. WOLA is regularly called upon for its research and analysis by policymakers, the media, and academics in the U.S. and Latin America. To further this work, WOLA gathers and publishes information about U.S. policies concerning Latin America, U.S. assistance (military or otherwise) to Latin American countries, and U.S. immigration practices, among other things.

161. WOLA engages in international and domestic internet communications that are essential to its mission. Among other things, WOLA's U.S.-based staff routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out WOLA's research, policy, and advocacy work.

162. WOLA's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of WOLA's communications and it violates WOLA's right to control those communications and the information they contain.

163. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates WOLA's international communications because WOLA is communicating with or about persons the government has targeted for Upstream surveillance. For instance, WOLA communicates with foreign government officials located abroad—including at times presidents and foreign ministers. Similarly, it communicates with policymakers, academics, journalists, human rights defenders, victims of human rights abuses, and staff from multilateral institutions, such as the Organization of American States, the Inter-American Development Bank, and the United Nations, some of whom are also likely targets. WOLA's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." WOLA communicates both with and about these likely targets. WOLA's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to WOLA's work.

164. Upstream surveillance undermines WOLA's ability to conduct its work. WOLA's research and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, WOLA has undertaken burdensome and costly measures to secure and protect its communications, including adopting more secure methods of electronic communication,

traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, WOLA believes that Upstream surveillance reduces the likelihood that policymakers, foreign government officials, experts, witnesses, and victims of human rights abuses will share sensitive information with WOLA's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

CAUSES OF ACTION

165. Upstream surveillance exceeds the authority granted by 50 U.S.C. § 1881a, and therefore violates 5 U.S.C. § 706.

166. Upstream surveillance violates the Fourth Amendment to the Constitution.

167. Upstream surveillance violates the First Amendment to the Constitution.

168. Upstream surveillance violates Article III of the Constitution.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs respectfully request that the Court:

1. Exercise jurisdiction over Plaintiffs' Complaint;

2. Declare that Upstream surveillance violates 50 U.S.C. § 1881a and 5 U.S.C. § 706;

3. Declare that Upstream surveillance is unconstitutional under the First and Fourth Amendments, and under Article III;

4. Permanently enjoin Defendants from continuing Upstream surveillance;

5. Order Defendants to purge all records of Plaintiffs' communications in their possession obtained pursuant to Upstream surveillance;

6. Award Plaintiffs fees and costs pursuant to 28 U.S.C. § 2412;

7. Grant such other and further relief as the Court deems just and proper.

Dated: June 19, 2015
Baltimore, Maryland

Respectfully submitted,

/s/ Deborah A. Jeon

Deborah A. Jeon
(Bar No. 06905)
jeon@aclu-md.org
David R. Rocah
(Bar No. 27315)
rocah@aclu-md.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

/s/ Patrick Toomey

Patrick Toomey
(pro hac vice)
ptoomey@aclu.org
(*signed by Patrick Toomey with permission of Debbie A. Jeon*)
Jameel Jaffer
(pro hac vice)
jjaffer@aclu.org
Alex Abdo
(pro hac vice)
aabdo@aclu.org
Ashley Gorski
(pro hac vice)
agorski@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

Charles S. Sims
(pro hac vice)

csims@proskauer.com
David A. Munkittrick
(pro hac vice)
dmunkittrick@proskauer.com
John M. Browning
(pro hac vice)
jbrowning@proskauer.com
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900