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

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Civil Action No. _____

Hon. _____

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;

ERIC H. HOLDER, in his 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
(admission pro hac vice pending)
ptoomey@aclu.org
Jameel Jaffer
(admission pro hac vice pending)
jjaffer@aclu.org
Alex Abdo
(admission pro hac vice pending)
aabdo@aclu.org
Ashley Gorski
(admission pro hac vice pending)
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
(admission pro hac vice pending)
csims@proskauer.com
David A. Munkittrick
(admission pro hac vice pending)
dmunkittrick@proskauer.com
John M. Browning
(admission pro hac vice pending)
jbrowning@proskauer.com
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900

March 10, 2015

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 hundreds of billions of 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 promote human rights, democracy, and social justice in Latin America. 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 Eric H. Holder 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 Holder is sued in his 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 2013, the government relied on the FAA to target 89,138 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. 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

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.

41. The NSA conducts Upstream surveillance by connecting surveillance devices to multiple major internet cables, switches, and routers 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.

42. 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.

43. 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, 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, 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, internet protocol ("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.

44. 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. 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.

Targeting and Minimization Procedures

45. 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.

46. 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.

47. 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

48. 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.

49. 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.

50. The 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.

51. 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.

52. 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.

53. 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.

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

55. 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.

56. 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.

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

Wikimedia Foundation

58. 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.

59. 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 412 and 495 million monthly visitors. On average, Wikimedia users visited Wikimedia "pages" or entries over 16 billion times each month during 2014. 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 or "discussion pages" to debate the editorial policies and decisions required for reliable and neutral content.

60. Other Projects include Wikimedia Commons, an online repository of free images, sound, and other media files; and Wikibooks, a platform for the creation of free textbooks and annotated texts that anyone can edit consistent with the policies of the site.

61. 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 movement; provides administrative support to grantees; organizes conferences and community-outreach events globally; and engages in advocacy on issues that affect the Wikimedia community—which, at its broadest level, consists of individuals who read or contribute to the work of the twelve Projects.

62. Upstream surveillance implicates at least two categories of Wikimedia communications: (i) Wikimedia communications related to the activities of its users, who read and edit Wikimedia's Projects and webpages, and who use them to interact with each other; and (ii) communications by Wikimedia staff.

63. As the operator of one of the most-visited websites in the world, Wikimedia engages in an extraordinarily high volume of internet communications. From October 2013 to October 2014, Wikimedia websites received over 248 billion page requests. Over the lifespan of the Wikimedia Projects, Wikimedia's users have edited its pages more than 2.3 billion times. More than 89 million registered and unregistered users have edited a Wikimedia page. Each of

these activities involves internet communications between Wikimedia and its users—the majority of whom are located abroad.

64. Indeed, Wikimedia engages in hundreds of billions of international communications each year. For a user to view, 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 the content of the requested webpage component to the user's device, where it is rendered and displayed to the user. In January 2015, Wikimedia's U.S.-based servers received and responded to over 62 billion HTTP or HTTPS requests from outside the United States.

65. Wikimedia also frequently engages in communications that permit its users to interact more directly, including one-on-one. 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.

66. Wikimedia's communications related to its users' activities 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.

67. 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.

68. Because of the sensitivity of this information, Wikimedia seeks to collect as little of it as possible. Where it does collect user 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 users, and it transmits a large volume of sensitive information about those users every day.

69. In addition to Wikimedia's communications related to its users' activities, as described above, Wikimedia engages in a second 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.

70. Wikimedia's communications—both communications related to the activities of Wikimedia's users and the communications of its staff members—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.

71. 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, 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.

72. Moreover, hundreds of billions of Wikimedia's international communications—its HTTP and HTTPS transmissions as well as its internal logs of user activity—contain details such as website addresses and IP addresses. For example, some Wikipedia pages contain the website addresses and domain names of foreign companies and organizations likely targeted for Upstream surveillance. 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.

73. 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.

74. 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.

75. 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 avoiding sensitive topics or forgoing communications altogether.

76. 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. The loss of these foreign users is a direct detriment to Wikimedia, its ability to receive information, 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.

National Association of Criminal Defense Lawyers

77. 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.

78. 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.

79. 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.

80. 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.

81. 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 gleaned from 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.

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

83. 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.

Human Rights Watch

84. 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.

85. 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.

86. 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.

87. 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.

88. 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

89. 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.

90. 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.

91. 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.

92. 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.

93. 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

94. 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.

95. 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.

96. 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.

97. 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.

98. 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

99. 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.

100. 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.

101. 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.

102. 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.

103. 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

104. 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.

105. 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.

106. 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.

107. 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.

108. 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

109. 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.

110. 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.

111. 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.

112. 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.

113. 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

114. WOLA is a non-profit, non-governmental organization based in Washington D.C. WOLA promotes human rights, democracy, and social justice by working with partners in Latin America and the Caribbean to shape policies in the United States and abroad. 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.

115. 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.

116. 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.

117. 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.

118. 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

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

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

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

122. 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: March 10, 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

Patrick Toomey
(admission pro hac vice pending)
ptoomey@aclu.org
Jameel Jaffer
(admission pro hac vice pending)
jjaffer@aclu.org
Alex Abdo
(admission pro hac vice pending)
aabdo@aclu.org
Ashley Gorski
(admission pro hac vice pending)
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
(admission pro hac vice pending)
csims@proskauer.com
David A. Munkittrick
(admission pro hac vice pending)

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