Written Remarks for the German Parliament Committee of Inquiry
September 8, 2016

Amie Stepanovich
U.S. Policy Manager and Global Policy Counsel
Access Now
https://accessnow.org

Thank you for the opportunity to provide evidence to the 1st Committee of Inquiry of the German Bundestag in the 18th electoral term. I appreciate the efforts of this Committee in pursuit of its mandate. Today, I would like to provide information on legislative, executive, and judicial actions since 2013 that have increased, or have created the capacity to increase, U.S. surveillance operations, and what those measures mean particularly for non-U.S. persons, including Germans citizens.

Access Now is a non-government organization that works to extend and defend the digital rights of users at risk around the world.[1] By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all. Access Now works from 10 locations around the world, including six offices. One of these offices is located in Washington, DC, where we engage directly on U.S. law and policy and its impact on users internationally.

Introduction

On June 6, 2013 the first documents obtained by Edward Snowden were published. This marked the beginning of a period where the public would receive unprecedented information on clandestine surveillance and intelligence operations in the U.S. and by its close partners around the world. For the first time, ordinary people were given a view into the world of "Prism," "Upstream," and "X-Keyscore," as well as "Muscular," "Bullrun," and "QuantumTheory."

In the U.S. these programs, and others, are authorized under a range of different authorities, separated by **the purpose of the surveillance** (criminal or national security), **the information to be collected** (metadata or content, for example), as well as **the target** and **the location of the surveillance** (foreign or domestic). While some of these authorities have safeguards built in to

[1] Access Now, https://www.accessnow.org.

protect against abuse -- a level of judicial authorization, congressional oversight, and public reporting, for example -- those safeguards largely do not apply to non-U.S. Persons.[2]

Herein I will briefly discuss the legal and technical means by which surveillance is conducted by United States officials. I will start by explaining the rights recognized by the United States and the extent those rights apply to non-U.S. persons. I will then give a short overview of the statutory structure that sits on top of these protections as well as unique issues that are raised in cross-border situations. In the final section I will explain the ways by which the U.S. seeks to ensure the technical ability to complete surveillance activities, including by compelling provider assistance, undermining encryption, and engaging in hacking operations.

The U.S. Constitution and Human Rights

All governments can and do conduct surveillance operations for the purposes of espionage. Absent additional restrictions, U.S. intelligence agencies are able to engage in any surveillance operations that do not run afoul of the protections provided in the U.S. Constitution. This includes the Fourth Amendment, which provides the cornerstone for the right to privacy in the United States. It states, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The application of the Fourth Amendment in the digital era is an evolving area of law. And while the scope of extraterritorial application of the Fourth Amendment is not entirely clear, it's generally accepted that it only extends outside the geographic United States to any extent for citizens, permanent residents, or others with a "substantial" connection.[3] In addition, the Foreign Intelligence Surveillance Court of Review has recognized an exception to the Fourth Amendment warrant requirement for foreign intelligence "when surveillance is conducted to

[2] A U.S. Person is a U.S. citizen, a permanent resident, an unincorporated entity with a significant number of members who are citizens or permanent residents, or a corporation incorporated into the United States, though the latter two categories are excluded if a foreign power. *See* 50 U.S.C. § 1801 (i).

[3] *See U.S. v. Verdugo-Urquidez*, 494 U.S. 259 (1990), *available at* http://caselaw.findlaw.com/us-supreme-court/494/259.html. *See also* Amy E. Pope, *Lawlessness Breeds Lawlessness: A Case for Applying the Fourth Amendment to Extraterritorial Searches* (Florida Law Review 2013), *available at* http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1170&context=flr; Steve Vladeck, *Cross-Border Shootings as a Test Case for the Extraterritorial Fourth Amendment*, Just Security (July 10, 2015), https://www.justsecurity.org/24541/cross-border-shootings-test-case-extraterritorial-fourth-amendment/; Orin Kerr, *Does the Fourth Amendment Allow Extraterriotiral State Search Warrants?*, the Volokh Conspiracy (Jan. 8, 2010), http://volokh.com/2010/01/08/does-the-fourth-amendment-allow-extraterritorial-state-search-warrants/.

obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States."[4]

While not identical, constitutional rights are largely coextensive with human rights recognized in international human rights documents, including the International Covenant on Civil and Political Rights ("ICCPR"). Both the U.S. Constitution and the ICCPR recognize rights to privacy, freedom of expression, and due process, though the standards for enforcing these rights differ slightly. For example, once an activity is shown to violate the human right to privacy, the activity can only be held consistent if it is both necessary and proportionate.[5] By contrast, in the U.S., a search falling within the Fourth Amendment tends to require probable cause to believe that evidence of a crime will be uncovered.[6]

The U.S. ratified the ICCPR in 1992,[7] though its position has consistently been that "the obligations assumed by a State Party to the [ICCPR] apply only within the territory of the State Party." As such, the activities of the U.S. intelligence community directed at non-U.S. persons outside of the United States is largely unlimited by either Constitutional limitations or human rights obligations.

U.S. Surveillance Legal Structure and Reform

In addition to the U.S. Constitution, the U.S. Congress has enacted several laws that provide greater protections for certain types of data. The primary laws are the Electronic Communications Privacy Act of 1986 ("ECPA") as well as the Foreign Intelligence Surveillance Act of 1979 ("FISA"). FISA has been amended and expanded several times, including by the USA PATRIOT Act of 2001 and the FISA Amendments Act of 2008 ("FAA"), Section 702 of the FAA provides authority for the infamous Prism and Upstream surveillance programs.[8] These

---

[4] Steve Vladeck, *Why Clapper Matters: The Future of Programmatic Surveillance*, Lawfare (May 22, 2012), https://www.lawfareblog.com/why-clapper-matters-future-programmatic-surveillance.

[5] The International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/ (last visited Sept. 5, 2016).

[6] This is true, though Courts hold the Fourth Amendment inapplicable except in cases where there exists a reasonable expectation of privacy, which does not includes instances, for example, where you have turned over the data to a third-party, which includes phone detail records. *See Smith v. Maryland*, 442 U.S. 735 (1979). Even when there is a reasonable expectation of privacy there are exceptions to the warrant requirement, such as searches incident to arrest and searches of automobiles, were lesser standards have been approved. *See, e.g., Terry v. Ohio*, 392 U.S. 1 (1967).

[7] The United States signed the Covenant on October 5, 1977, and ratified it on June 8, 1992. *See* United Nations Office of the High Commissioner on Human Rights, Status of Ratification (Interactive) http://indicators.ohchr.org/ (last visited Sept. 6, 2016)..

[8] *See* Cindy Cohn, *Word Games: What the NSA Means by "Targeted" Surveillance Under Section 702*, EFF Deeplinks (Aug. 24, 2016), https://www.eff.org/deeplinks/2016/08/nsa-word-games-mass-v-targeted-surveillance-under-section-702.

laws deal with surveillance in the context of criminal proceedings (ECPA) and national security (FISA). However, these laws also come with limitations: the protections are largely geographically limited to surveillance that takes place within the United States, and, at least in the case of ECPA, the legislation is far out of date leaving huge loopholes in the protections it is meant to provide.

The laws are also vague, confusing, and arguably open to broad interpretation. Several words used in U.S. surveillance law are "terms of art" or have non-obvious meanings. For example, "bulk surveillance" means not "large" surveillance but indiscriminate surveillance which is not keyed to a target, however large that target may be.[9] In addition, the definition of "collection" explicitly excluded "information that only momentarily passes through a computer system," allowing the wholesale scanning of internet traffic before certain protections set in.[10]

Some terms of art may also have secret definitions which render their meaning unknowable by the public. This is exactly what that first Snowden document revealed: that the Foreign Intelligence Surveillance Court (the "FISC"), the secret court established to approve surveillance requests under FISA authority, had approved surveillance under a provision in FISA which authorized the collection of records only when they were "relevant to an authorized investigation." However, the government argued, and the FISC agreed, that the standard should be re-defined to permit collection of *all* phone records transiting the United States. That revelation from Mr. Snowden led to several court challenges, and the eventual passage of the USA FREEDOM Act, passed in June 2015 to rebut the FISC's interpretation, as well as to reform other provisions and allow for increased transparency and accountability around NSA surveillance. Unfortunately, while the reforms in the USA FREEDOM Act extend to all persons regardless of citizenship, the law did not substantively reform the other FISA authorities targeted specifically at non-U.S. persons.

The final major grant of surveillance authority is Executive Order ("EO") 12333. Signed by President Ronald Reagan in 1981, EO 12333 speaks to international surveillance, primarily foreign intelligence and counterintelligence.[11] While there are some limitations in EO 12333, it

[9] *See, e.g.*, U.S. National Security Agency, PPD-28 Section 4 Procedures (Jan. 12, 2015), *available at* https://www.dni.gov/files/documents/ppd-28/NSA.pdf, fn 1 at 7.
[10] U.S. Department of Defense, DoD Manual 5240.01: Procedures Governing the Conduct of DoD Intelligence Activities (Aug. 8, 2016), *available at* https://www.documentcloud.org/documents/3009803-DoD-Manual-5240-01-20160808.html at 45.
[11] "Foreign intelligence" is defined as "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities." EO 12333 § 3.4 (d). Compare to the definition of "foreign intelligence" information in the FISA, which includes "(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against— (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of

essentially allows any surveillance that is not otherwise unconstitutional or unlawful. The most major step to limit EO 12333 was the implementation of Presidential Policy Directive ("PPD") 28.[12] In addition to the USA FREEDOM Act, PPD 28 is the other primary surveillance reform enacted following the Snowden revelations.

The Directive was an unprecedented U.S. statement on human rights of non-U.S. persons. As explained above, the U.S. has not recognized the extraterritorial reach of human rights instruments like the ICCPR. However, PPD 28 establishes that, "all persons have legitimate privacy interests in the handling of their personal information."

Despite the huge step forward taken in the issuance of PPD 28, its actual or long-term impact may be limited. For example, as Access Now noted after the U.S. Office of the Director of National Intelligence ("ODNI") released its first interim report:

> *Notably, even those few mandated additional protections enumerated in the ODNI Report are frustrated by exceptions and caveats. Perhaps the most important instance of this is the frequent declaration that, "it is important that elements [of the intelligence community] have the ability to deviate from their procedures when national security requires doing so," which renders large chunks of the Report laughably meaningless. The absence of ongoing reporting requirements exacerbates the problem, failing to provide the public oversight and transparency mechanisms necessary for real reform.*[13]

Since then, intelligence agencies have published further documents on implementation of PPD 28.[14] While the documents do show a step toward recognition of the rights of non-U.S. persons, they also continue to feature several caveats and exceptions. Finally, it is perhaps most noteworthy that any additional protections implemented under PPD 28 are, as the name of the document suggests, based in policy and not in law, and therefore can be modified or removed without public debate by this or any future administration.

---

mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to— (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801 (e). "Counterintelligence" is "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs." EO 12333 § 3.4 (a).

[12] The White House, Presidential Policy Directive -- Signals Intelligence Activities (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[13] Jack Bussell, *Interim Report Fails to Provide Protections for Non-U.S. Persons*, Access Now Blog (Oct. 21, 2014) https://www.accessnow.org/interim-report-fails-to-provide-protections-for-non-us-persons/.

[14] *See* Office of the Director of National Intelligence: IC on the Record, Signals Intelligence Reform: 2015 Anniversary Report https://icontherecord.tumblr.com/ppd-28/2015/overview, last visited Sept. 6, 2016.

Cross-Border Surveillance and Agreements

In addition to surveillance conducted by U.S. intelligence agencies to fulfill their own missions, there are several different agreements used to authorize the transmission of surveillance information back and forth between different governments and jurisdictions. Many of these agreements often are formed and operate behind a veil of secrecy, with neither transparency nor accountability to the public.

Law enforcement transfers of data are made under several mechanisms. The most common are Mutual Legal Assistance Treaties ("MLATs"). MLATs are agreements between two or more countries that create obligations with the status of international law for governments to assist one another in criminal investigations and prosecutions. Law enforcement officers or prosecutors use them when they need help to obtain evidence from within another country's jurisdiction. Letters rogatory have traditionally served the same purpose, though they are procedurally outdated and have been replaced by MLATs in many settings. MLATs bring with them several problems, among which that they are infamously slow.[15] Because of this, despite that MLATs may in many instances be the most rights-protective means for cross-border requests for user data, governments often try to find loopholes and other means to bypass their procedures.[16]

Recently, the U.S. government has proposed legislation that would allow for countries that it designates to bypass the MLAT process outright and directly request data from U.S. companies or place wiretaps. Countries that enter into agreements with the U.S. under this law would have to provide reciprocal access. While this process would inevitably speed up the MLAT process for some, the current draft legislation fails to adequately protect human rights in several ways.[17] One of these is that it extends the reach of countries with overly invasive surveillance laws, like the United Kingdom. The UK is imminently set to approve its Investigatory Powers Bill, which provides broad authority for surveillance, including bulk surveillance and bulk hacking directed outside of the UK. While the UK's agreement with the U.S. would, under the U.S. law, have to provide some additional, albeit inadequate, protections for U.S. persons against UK spying, there would be no additional protections for users from other countries, like Germany.

---

[15] *See* Drew Mitnick, *the Urgent Need for MLAT Reform*, Access Now Blog (Sept. 12, 2014) https://www.accessnow.org/the-urgent-needs-for-mlat-reform/; *see also* Mutual Legal Assistance Treaties, https://MLAT.info (last visited Sept. 6, 2016)..

[16] *See* Drew Mitnick, *In Failing to Honor its Obligations for International Legal Assistance, U.S. Harms All Users*, Access Now Blog (Apr. 28, 2015) https://www.accessnow.org/us-failing-to-honor-its-obligations-for-international-legal-assistance/.

[17] *See* Drew Mitnick, *Four Ways the New Proposal for Bypassing MLATs Fails Human Rights*, Access Now Blog (July 20, 2016) https://www.accessnow.org/four-ways-new-proposal-bypassing-mlats-fails-human-rights/.

Another cross-border data agreement is the Umbrella Agreement. The Agreement does not provide for transfers of data, but instead aims to establish common standards that must be in place for data transfers between the EU and the U.S. in the context of criminal and terrorism matters. For example, the text sets rules for data retention periods, onward transfer to third states, right to access and rectification, and notification in case of data breach.[18]

Unfortunately, the passage of the Judicial Redress Act in the U.S. was established as the only pre-requisite before the agreement could be finalized. While the initial version of the Judicial Redress Act was a positive step which would have marginally increased the rights of Europeans in the U.S., the version that was passed was gutted before becoming law.[19] The version of the Judicial Redress Act that was signed by President Obama not only fails to comply with the EU Charter of Fundamental Rights, it also undermines the ability of Europeans to call for the U.S. to protect their human rights in regard to government surveillance. Any country deemed to have "impede[d] the national security interests of the United States" would be ineligible for status.[20] This language was specifically inserted in response to the negotiations between the EU and the U.S. on the "Privacy Shield," which replaced the Safe Harbor Arrangement after the Court of the Justice of the European Union ("CJEU") held that it violated EU law for failure to protected personal data of EU citizens against U.S. surveillance.[21] The enacted Judicial Redress Act severely limits the ability of the EU to negotiate for additional protections for EU data without risking their hard-fought redress rights.

Outside of the law enforcement context, several agreements exist to also handle transfers of national security information. The primary agreement is known as the "Five Eyes" in reference to the five country parties -- the U.S., UK, Canada, Australia, and New Zealand. The agreement is very secretive. Here, Privacy International explains what little we know about the agreement:

> *"...under the agreement interception, collection, acquisition, analysis, and decryption is conducted by each of the State parties in their respective parts of the globe, and all intelligence information is shared by default. The agreement is wide in scope and establishes jointly-run operations centres where operatives from multiple intelligence agencies of the Five Eyes States work alongside each*

[18] *See* Access Now Policy Team, *What the E.U.-U.S. Umbrella Agreement Does -- and does not -- Mean for Privacy*, Access Now Blog (Sept. 10, 2015) https://www.accessnow.org/what-the-eu-us-umbrella-agreement-does-and-does-not-mean-for-privacy/.
[19] *See* Estelle Massé, *Five Things You Should Know About the EU-US Umbrella Agreement*, Access Now Blog (Sept. 24, 2015) https://www.accessnow.org/five-things-you-should-know-about-the-eu-us-umbrella-agreement/.
[20] *See* Press Release: EU Council Greenlights Umbrella Agreement, but Parliament Hasn't Given Final Consent Yet, Access Now (June 2, 2016) https://www.accessnow.org/eu-council-greenlights-umbrella-agreement-parliament-hasnt-given-final-consent-yet/.
[21] *See* Press Release: E.U. and U.S. reach deal on new Safe Harbor data-transfer arrangement, Access Now (Feb. 2, 2016) https://www.accessnow.org/13871-2/.

other. Further, tasks are divided between SIGINT agencies, ensuring that the Five Eyes alliance is far more than a set of principles of collaboration. The level of cooperation under the agreement is so complete that the national product is often indistinguishable."[22]

Agreements like the Five Eyes compound human rights invasions of individual governments by providing for opaque collaborations and data sharing. In addition, as Privacy International further points out, the Five Eyes is only the tip of the iceberg, and other agreements include the Nine Eyes, the Fourteen Eyes (including Germany), the Forty-One Eyes, the Club of Berne, and the Counterterrorist Group, among others.[23] Far too little is known about any of these agreements, which ostensibly operate as shadow surveillance law for users around the world.

Going Dark and the Quest for Exceptional Access

Equally as important as the U.S. legal authorities to conduct surveillance are the steps taken by the U.S. to ensure that they can access all of the information they seek. Two separate routes are currently available in U.S. law to facilitate assistance with surveillance operations. The first are so-called "provider assistance provisions" codified in several provisions in both ECPA and FISA. These provisions compel providers to furnish "all information, facilities, [and/or] [technical] assistance necessary" to assist with surveillance activities.[24] Additionally, in 1994, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA") which

[22] Privacy International, the Five Eyes, https://www.privacyinternational.org/node/51 (last visited Sept. 6, 2016), also linking to publicly available documentation of the Five Eyes agreement.
[23] *Id*.
[24] *See, e.g.*, 50 U.S.C. § 1802 (a)(4)(A) ("furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers"); 50 U.S.C. § 1861 (c)(2)(F)(vi) ("direct each person the Government directs to produce call detail records under the order to furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production"); 50 U.S.C. § 1881b (c)(5)(B) ("if applicable, an electronic communication service provider to provide to the Government forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition"); 50 U.S.C. § 1842 (d)(2)(B)(i) ("upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned"); 18 U.S.C. § 2518 (4) ("a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted.").

mandates that telecommunications companies build their systems so that they are "wiretappable."[25]

But, increasingly, personal data and communications have moved onto the internet. This move has largely given law enforcement and national security agencies easier access to more information than ever before. However, as companies and users have adopted increased encryption standards and protocols, government officials have been prevented from gaining access to some of the information, at least without the assistance of one of the parties to the conversation. Notably, the increase in encryption has largely been seen by experts as a positive step. UN Special Rapporteur David Kaye has explained: "encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age."[26] Undermining encryption would also undermine human rights, and as well as "force a U-turn from the best practices now being deployed to make the Internet more secure," "substantially increase system complexity" and raise associated costs, and "create concentrated targets that could attract bad actors."[27]

Both provider assistance provisions and CALEA have limited application in regard to encryption. CALEA specifically does not apply to information services.[28] In addition, CALEA contains a carve-out for encryption that was implemented by a subscriber or customer.[29] The provider assistance provisions generally require that the surveillance is "necessary" and require that it is unobtrusive. As such, no law in the United States currently limits the types of encryption that can be developed or implemented by internet or messaging companies.[30]

---

[25] *See* 47 U.S.C. § 1002.
[26] *See* United Nations Office of the High Commissioner on Human Rights, Report on encryption, anonymity, and the human rights framework, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (last visited Sept. 6, 2016) (linking to the full report).
[27] Secure the Internet, https://securetheinternet.org/ (last visited Sept. 6, 2016), citing Peter G. Neumann, et al, *Inside Risks: Keys Under Doormats*, Viewpoints (Oct. 2015), *available at* http://www.csl.sri.com/users/neumann/cacm237.pdf.
[28] "The requirements of subsection (a) do not apply to -- (A) information services…" 47 U.S.C. § 1002 (b)(2)(A). The term "information services"— (A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and (B) includes— (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services; but (C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network. 47 U.S.C. § 1001 (6).
[29] "A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." 47 U.S.C. § 1002 (b)(3).
[30] The U.S. still has regulations on the export of certain types of encryption, but that is outside the scope of this testimony.

However, U.S. law does intervene with encryption in other ways. For example, U.S. law requires the National Institute for Standards and Technologies ("NIST"), the key agency in the United States for developing encryption standards, to consult with the NSA in the process of development.[31] The consultation has ensured that NIST had the best technical experts and cryptographers in government available as resources. However, over time it has raised suspicion (and even outright accusation) as the NSA's surveillance mission has further and further intruded upon its separately-established Information Assurance mission.[32] Compromised encryption standards would make it easy to bypass otherwise strong protections. Recently, Admiral Michael Rogers, the director of the NSA, announced a reorganization of the NSA which will instead further conflate these distinct missions and raises increased suspicion of U.S.-developed encryption standards. While a NIST guidance document is being established, it allows for loopholes for NSA influence.[33]

Certain U.S. officials have called for legislation, regulation, or voluntary action on the part of companies to directly weaken encryption in order to allow for government access, specifically access that has already been authorized under the relevant law. The U.S. Department of Justice brought a lawsuit against Apple, Inc. earlier this year to compel the design of a new iPhone operating system that would bypass standard security measures necessary for the phone's encryption. That case was withdrawn after the FBI leased an exploit from a private vendor to break into the phone directly. James Comey, the FBI's director, has also testified to Congress that the FBI is "going dark," the term used since 2010 to describe the loss of surveillance information because of encryption. This testimony led to the drafting of the Compliance with Court Orders Act of 2016 ("CCOA"), which, if passed would practically bar companies from implementing end-to-end encryption or device encryption.[34] Finally, Director Comey and several other government officials have held private meetings with the heads of major technology companies to discuss this topic, presumably to try to reach a private agreement to maintain access to data. It is unclear what topics were covered in those meetings.

---

[31] *See*, 15 USC § 278g-3. *See also* Memorandum of Understanding between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235, *available at* http://csrc.nist.gov/groups/ST/crypto-review/documents/NIST_NSA_MOU-1989.pdf (last visited Sept. 6, 2016); Memorandum of Understanding between the Director of the NAtional Institute of Standards and Technology (NIST) and the Director of the NAtional Security Agency (NSA) Concerning the Implementation of the Federal Information Security Management Act of 2002, *available at* http://csrc.nist.gov/groups/ST/crypto-review/documents/NIST_NSA_MOU-2010.pdf (last visited Sept. 6, 2016).

[32] *See* Amie Stepanovich, *Virtual Integrity: Three Steps Toward Building Stronger Cryptographic Standards*, Access Now Blog (Sept. 18, 2016), https://www.accessnow.org/virtual-integrity-the-importance-of-building-strong-cryptographic-standards/.

[33] *See* Amie Stepanovich, *New Crypto Guidance Draft Offers Brighter Path Forward*, Access Now Blog (Jan. 29, 2015) https://www.accessnow.org/new-crypto-guidance-draft-offers-brighter-path-forward/.

[34] *See* Discussion Draft: Compliance with Court Orders Act of 2016, *available at* https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf (last visited Sept. 6, 2016).

These efforts to undermine encryption are ongoing. Just last week, Director Comey indicated that he intended to keep pushing for encryption mandates into 2017.[35] However, even without directly undermining encryption, the U.S. government has other options available. In fact, we know that U.S. agents have exploited vulnerabilities in computer systems for decades, a process known as hacking. The National Security Agency's (NSA) Office of Tailored Access Operations has been active since the late-1990s.[36] Similarly, the Federal Bureau of Investigation (FBI) has engaged been hacking users since at least the early 2000s.[37]

Currently pending in U.S. Congress is an amendment to U.S. Federal Rule of Criminal Procedure 41. The amendment was approved by the U.S. Supreme Court earlier this year and will go into effect automatically unless expressly withdrawn or postponed by an act of Congress. Currently, magistrate judges in the United States can only issue a warrant for a search within his or her jurisdiction. Rule 41 establishes a few exceptions to this, and the amendments would create an additional exception for government hacking operations when the target of the operation has concealed his or her location via technological means or in certain other computer investigations, largely related to searches of devices that have fallen victim to what is known as a "botnet" attack. In practical application, this rule change will allow a judge to issue a warrant to search computers located anywhere in the world, including in Germany, so long as the government does not know where that location is. This expansion, along with the lack of statutory authority or safeguards directly addressed at government hacking, will greatly open up the possibility for some of the most invasive surveillance operations conducted by law enforcement, and it is being done outside of Congress and with minimal public debate.

Conclusion

Access Now advocates for the rights of users at risk around the world. To do that, we support the position that all users have human rights which should be recognized and respected. The internet has eliminated major barriers to communication, allowing global connections regardless of geographic borders. However, these borders remain significant for deciding when, how, and with what safeguards the United States can conduct surveillance operations. And the U.S. is not alone

[35] *See* Eric Tucker, *Comey: FBI Wants 'Adult Conversation' on Device Encryption*, AP (Aug. 30, 2016), http://bigstory.ap.org/article/7d57f576e3f74b6ca4cd3436fbebf160/comey-fbi-wants-adult-conversation-device-encryption.
[36] *See* Kim Zetter, *NSA Hacker Chief Explains How to Keep Him Out of Your System*, Wired (Jan. 28, 2016) https://www.wired.com/2016/01/nsahackerchiefexplainshowtokeephimoutofyoursystem/; Video: USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers (Jan. 28, 2016), *available at* https://www.usenix.org/conference/enigma2016/conferenceprogram/presentation/joyce.
[37] *See* Kim Zetter, *Everything We Know About How the FBI Hacks People*, Wired (May 15, 2016) https://www.wired.com/2016/05/history-fbis-hacking/; https://www2.fbi.gov/hq/otd/otd.htm.

in this matter. Countries around the world, from China to France and the United Kingdom, even Germany, have conducted intrusive surveillance operations which are disproportionately targeted at users outside their borders and are seeking additional authority to do so.[38] We oppose all of these efforts and call on governments to act together to respect human rights, even as they pursue legitimate surveillance operations. This must start with a holistic review of all available authorities and programs, as opposed to targeted reviews, to determine the full impact of these operations on human rights.

Thank you for your time. If you have additional questions you can reach me at amie@accessnow.org.

[38] *See, e.g.*, Andre Meister, *Secret Report: German Federal Intelligence Service BND Violates Laws and Constitution by the Dozen*, Netzpolitik.org (Sept. 2, 2016), https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/; Lucie Krahulcova and Drew Mitnick, *UK's IP Bill: deficient on privacy protections, ample on surveillance authority*, Access Now Blog (Mar. 3, 2016) https://www.accessnow.org/14341-2/; Estelle Massé, *After the Paris attacks, France enacts sweeping legislation limiting fundamental freedoms*, Access Now Blog (Nov. 25, 2015), https://www.accessnow.org/after-the-paris-attacks-france-enacts-sweeping-legislation-limiting-fundamental-freedoms/.