Introduction, Background and Framework

1. The Brennan Center for Justice at NYU School of Law,[1] Access, the American Civil Liberties Union, the Center for Democracy and Technology, Electronic Frontier Foundation, Electronic Privacy Information Center (EPIC), Human Rights Watch and PEN American Center make this submission to the Human Rights Council in preparation for the 2015 Universal Periodic Review of the United States of America.

2. During the 2010 Universal Periodic Review, the U.S. accepted in part two recommendations related to privacy and surveillance: first, that it legislate "appropriate regulations to prevent the violations of individual privacy" and "constant intrusion [into] … [and] eavesdropping of communications;"[2] and second, that it "guarantee the right to privacy and stop spying on its citizens without judicial authorization."[3] The U.S. assured the Human Rights Council that "[o]ur Constitution and laws contain appropriate rules to protect the privacy of communications," and pledged that "we collect information about our citizens only in accordance with U.S. law and international obligations."[4]

3. Since that review, it has been revealed that the U.S. government has been **secretly sweeping up massive amounts of digital communications and personal data of people around the world**. **Many of these programs operate with little meaningful oversight from either the judiciary or legislature.** Such indiscriminate surveillance, coupled with a systematic lack of transparency and oversight, amounts to a breach of Article 17 of the International Covenant on Civil and Political Rights ("ICCPR"), which prohibits arbitrary and unlawful interference with an individual's privacy or correspondence. U.S. surveillance activities discussed below also impair the exercise of other human rights, including the freedom of expression under Article 19 of the ICCPR, and the right of peaceful assembly under Article 21 of the ICCPR. For the same reasons, these surveillance activities also violate the rights to privacy, freedom of expression, and the freedom of peaceful assembly and association under Articles 12, 19 and 20 of the Universal Declaration of Human Rights ("UDHR") respectively. The chronic inability of both Americans and non-Americans to secure a meaningful remedy for unlawful or unconstitutional U.S. surveillance activities also violates their right to an effective remedy for human rights violations under Article 2(3) of the ICCPR and Article 8 of the UDHR.

4. This submission provides an overview of mass electronic surveillance activities conducted by the U.S. in the name of foreign intelligence gathering, and outlines the deficiencies in the domestic legal framework governing these activities, as well as inconsistencies with international human rights law. It also discusses recent attempts at

domestic reform, and how they continue to fall short of the U.S.'s international human rights obligations.

5. **Based on this analysis, we propose that the U.S. should:**

   i. Unambiguously recognize that its duty under human rights law to respect the privacy of individuals applies extraterritorially;

   ii. In the context of foreign intelligence gathering, collect, process, analyze, use, retain or disseminate digital communications and data only when it is necessary for the protection of specifically articulated U.S. national security interests, and only in a manner that produces the least intrusion on rights necessary to secure those interests;

   iii. Publish any official legal or policy document that contains significant legal interpretations of the U.S.'s surveillance laws and orders, with only those redactions that are truly necessary to protect legitimate national security interests; and

   iv. Reform current procedural laws and establish appropriate remedial mechanisms to ensure that both U.S. and non-U.S. persons affected by U.S. foreign intelligence surveillance operations is capable of obtaining effective remedies for privacy violations arising from such operations.

I. The State of U.S. Mass Surveillance of Digital Communications and Data Worldwide[*]

6. Classified documents leaked by former National Security Agency ("NSA") contractor Edward Snowden reveal that the U.S. government has been secretly collecting and monitoring potentially billions of electronic communications around the world. While the full extent of the NSA's surveillance operations is not known, what is known is sufficient to raise serious concerns. For example:

   i. *Bulk collection of telephone and other records*: The NSA has been collecting records of millions of calls within the United States under Section 215 of the USA PATRIOT Act.[5] While these records do not contain the contents of the calls, they include highly sensitive information such as the numbers that were dialed, call

[*] This submission does not discuss the surveillance of communications content within the U.S. that is conducted with a judicial finding of probable cause that the target of surveillance is an agent of a foreign power. *See* 50 U.S.C. § 1805.

duration and information about the time and date of the call, which are especially invasive since they are gathered over time and aggregated with the information of many others.[6] The NSA has also admitted that, for several years, it collected e-mail and Internet records in bulk under Section 402 of the Foreign Intelligence Surveillance Act ("FISA"),[7] but claims that it has since discontinued this program due to operational – but not legal – considerations.[8]

ii. *Collection of telephone and internet communications inside the United States*: Under Section 702 of FISA, the NSA collects the telephone and internet communications of non-U.S. persons[9] reasonably believed to be outside the U.S. that are stored or transmitted within the U.S.[10] Two large-scale Section 702 collection programs have been revealed. Under a program code-named UPSTREAM, the NSA copies communications and data passing through networks that connect North America to the rest of the world.[11] Under a second program code-named PRISM, the government collects information stored in the U.S. from major U.S.-based internet companies, such as Google, Facebook and Apple.[12] As of April 2013, there were an estimated 117,675 active surveillance targets in PRISM's counterterrorism database.[13]

iii. *Collection of telephone and internet communications outside the United States*: The NSA also collects telephone and internet communications from locations outside the United States under Executive Order ("EO") 12333. While much about the operations conducted under the order remain secret, it has been used to justify unprecedentedly broad surveillance. For example, pursuant to EO 12333, the U.S. government reportedly collects and stores for thirty days a recording of every single call made in or out of at least *two entire countries*, including the Bahamas.[14] The government apparently intends to expand the program—called MYSTIC—to more countries, if it has not already.

iv. *Collection of communications data outside the United States:* The NSA also sweeps up communications data (e.g., e-mail address books and contact lists) outside the United States through methods such as tapping into fiber optic cables that connect the data centers of major Internet companies around the world.[15] For example, under a program code-named MUSCULAR, the NSA and the UK intelligence agency GCHQ reportedly tap into internal Yahoo and Google networks to collect data from hundreds of millions of user accounts.[16] This data is temporarily held in a digital "buffer," and sent through a series of filters to "select" information the NSA wants. Between December 2012 and January 2013, the NSA "selected" and sent back to its headquarters 181,280,466 new records of communications data.[17] Programs like MUSCULAR also operate pursuant to EO

12333, which authorizes the interception of signals to collect information for a broad range of "foreign intelligence purposes."[18] There is little doubt that such activities impact the communications and privacy of a large proportion of the world's population. Recent statements from a former U.S. official confirm this.[19]

7. In the context of the ICCPR, the U.S. government has in recent years taken the position that its human rights obligations – including its duty to respect privacy and the freedom of expression – do not extend to non-U.S. persons located beyond its territorial borders.[20] This position is inconsistent with the statements of the Human Rights Committee and the Office of the United Nations High Commissioner for Human Rights ("OHCHR"), which affirm that states are required to respect and ensure the right to privacy of not only persons within their territory, but also of those who are within their "power or effective control."[21]

8. The communications and data belonging to millions of non-U.S. persons located abroad flow across U.S. borders on a daily basis and are within the "power and effective control" of the U.S. Many of the world's biggest Internet companies (such as Google, Facebook and Apple) are based in the U.S., and much of their customers' communications and data are stored within U.S. territory, subject to U.S. legal process. Much of the world's digital communications and Internet data also flow through fiber optic cables located in U.S. territory, even if they are not stored there. Interception within the U.S. can capture all of this information.

9. As for the interception of communications and data outside the U.S., it is a well-established principle of international law that "a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking "at home"."[22] The U.S. government intercepts millions of communications that are wholly transmitted and stored abroad. The government also asserts jurisdiction over user data held by U.S. Internet companies even if such data is stored outside the U.S. Such communications and data – much of which concern non-U.S. persons abroad – are thus also within the "power and effective control" of the U.S.

10. Intelligence partnerships significantly extend the global reach of U.S. surveillance activities. The U.S. is part of an intelligence sharing alliance with Australia, Canada, New Zealand and the United Kingdom known as the "Five Eyes."[23] Members intercept, collect, analyze, translate and decrypt signals intelligence data in their respective parts of the world and share them with the others,[24] and sometimes also collaborate on specific surveillance programs. For example, the NSA has reportedly partnered with the U.K's intelligence agency GCHQ to access massive volumes of phone calls and Internet traffic that pass through fiber optic cables located in the U.K,[25] and to crack or circumvent

encryption technologies.[26] The NSA's intelligence partnerships also transcend the "Five Eyes." For example, the Snowden documents reveal that the NSA has shared large volumes of raw private data with Israeli intelligence, including transcripts of telephone and online communications, voice clips, facsimiles and telephony metadata concerning both U.S. and non-U.S. persons. [27]

II. Mass Government Collection of Communications and Data is Arbitrary and Unlawful

11. Following the Snowden revelations, the U.S. government has conceded that several of its surveillance programs, including the phone records program and the former internet metadata program, involve the bulk acquisition of communications data.[28] However, the government has repeatedly justified these programs on the basis that it does not "collect" information in a way that interferes with an individual's privacy until it has processed or analyzed that information. Notably, a key intelligence policy directive states that "[d]ata acquired by electronic means is 'collected' only when it has been processed into intelligible form."[29] In accordance with this theory, since privacy protections are only triggered upon this definition of "collection," the NSA can acquire and store vast amounts of digital communications and data without legal constraint until it processes that data.

12. This position is inconsistent with international human rights law, which considers the acquisition and copying of personal information an "interference" with the right to privacy. The Human Rights Committee's General Comment 16 states that the act of "*gathering and holding* … personal information on computers, databanks and other devices" must be "regulated by law."[30] This principle is consistent with the European Court of Human Rights' recognition that the "storing by a public authority of information relating to an individual's private life amounts to an interference" with the right to privacy, regardless of whether the stored information is subsequently used, processed or analyzed.[31] The OHCHR affirmed this principle in its recent report on the right to privacy in the digital age.[32]

13. Government collection of digital data violates the right to privacy under Article 17 of the ICCPR if it is "arbitrary and unlawful." The OHCHR, the UN Special Rapporteur the promotion and protection of human rights and fundamental freedoms while countering terrorism and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression have affirmed that any interference with privacy must be provided by law, necessary to accomplish a legitimate aim, and proportionate to the aim sought.[33] The mass acquisition of communications and data around the world without

proof that such information is necessary for the protection of national security and without other safeguards is by its very nature arbitrary and indiscriminate.

14. The U.S. government has also defended other large-scale collection programs like UPSTREAM and MUSCULAR as "targeted" and non-arbitrary. Under the UPSTREAM program conducted under Section 702 of FISA, the NSA makes a copy of *every* electronic and text communication passing through U.S. borders, then applies selectors to this trove of data to select communications for longer-term storage.[34] Under the MUSCULAR program conducted under EO 12333, data siphoned from fiber optic cables worldwide are directed into a "buffer," and then sent through a series of filers to "select" information the NSA wants.[35]

15. Although the government "temporarily" acquires and copies *all* the data passing through vast communications streams under these programs, it argues that it engages in "targeted collection" because it applies selectors to identify information for longer-term storage and analysis. Notably, under Presidential Policy Directive 28 ("PPD-28"), the latest intelligence directive issued by the President in response to Snowden's revelations, the government has relied on this theory to exclude programs it deems to be "targeted collection" from the Directive's limits on the uses of signals intelligence data.[36]

16. That the government's uses selectors in these programs does not alone ensure meaningful privacy. Under Section 702 of FISA, a surveillance "target" may be any foreigner abroad, whether suspected of wrongdoing or not. A "target" could be a foreign journalist, dissident or human rights defender. Moreover, Section 702 permits the NSA to target large groups, such as "al-Qaeda" or "al-Shabab." and the government has stated that its selector terms can include phone numbers, e-mail addresses and other identifiers of any person thought to be associated with such groups. Selectors are applied to collect not only communications to and from the NSA's "foreign" targets, but also communications *about* the targets that merely mention such terms. [37] Accordingly, the NSA may sweep up and store indefinitely[38] thousands of e-mails that simply mention an identifier associated with a member of "al-Shabab," even if they are, among other things, simply discussing U.S. counterterrorism policy or a recent news story. Under EO 12333, the government may be intercepting an even larger number of communications with little or no intelligence value, since selectors could theoretically be as broad as names or general descriptions like "Pakistani Taliban" or "al-Shabab."[39]

17. In any case, the permissible justifications for surveillance of non-U.S. persons are far too broad. Under Section 702 of FISA, the U.S. can "target" non-U.S. persons reasonably believed to be outside the U.S. to acquire "foreign intelligence information." However, the definition of foreign intelligence information goes beyond what is necessary to

protect national security, to also include communications or data that merely relates to the conduct of U.S. foreign affairs.[40] Under EO 12333, the government can collect an even broader range of "foreign intelligence," which is defined under the Order as any information relating to the capabilities, intentions or activities of foreign organizations or foreign persons, regardless of whether they are associated with foreign governments or international terrorists or present any threat.[41] Such open-ended definitions of "foreign intelligence" allow the NSA to sweep up massive amounts of communications and data in violation of the standards of necessity and proportionality.

III. Mass Collection of Metadata is a Violation of Privacy

18. The U.S. government frequently relies on the distinction between content and metadata (essentially non-content information that describes a communication, such as call logs, the numbers dialed, and the time and date of a call) to justify metadata surveillance programs that can reveal intimate details about a person's associations and activities. In the 1970s, the Supreme Court, the nation's highest court, found that individuals had no "reasonable expectation of privacy" in the phone numbers they dialed because they had knowingly revealed them to a third party telecommunications provider in the course of making a phone call.[42] The government has since pursued an aggressive reading of this 'third party' doctrine to justify the Section 215 program, and the large-scale collection of metadata generally without a warrant.

19. The government's claim that metadata is entitled to diminished privacy protection is inconsistent with emerging international principles and is increasingly questioned in U.S. courts as well. The OHCHR observed in its 2014 report on digital privacy that "[t]he aggregation of information commonly referred to as "metadata" may give an insight into an individual's behavior, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication."[43] The European Court of Justice echoed this observation in a recent decision striking down an EU directive mandating the retention of communications data, observing that such data "may allow very precise conclusions to be drawn concerning the private lives of the persons."[44]

20. Recent U.S. Supreme Court decisions affirm the privacy interest in metadata, and cast doubt on the validity of the "third party" doctrine, especially as it relates to bulk collection. Although the Court has not directly addressed the issue, it has observed that non-content information such as cell phone location data is highly private since it "can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[45] And in a 2012 decision finding that the police's GPS

monitoring of a suspect without a warrant is unconstitutional, one Justice stated that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" in an age where "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[46]

IV. Systemic Lack of Judicial Oversight of U.S. Foreign Intelligence Surveillance Operations

21. The Foreign Intelligence Surveillance Court, or FISC, is the main judicial body that oversees foreign intelligence surveillance operations. As a threshold matter, however, a large swath of intelligence activity is simply not overseen by the FISC. Surveillance under EO 12333 – though breathtaking in scope – is not within the jurisdiction of the FISC. The executive alone determines the regulations that govern its surveillance under the executive order. Even for surveillance conducted inside the United States under Section 702 of FISA, the FISC's role is narrowly circumscribed. The FISC approves so-called "targeting" and minimization" procedures, but these procedures provide extremely limited protections for the privacy of U.S. persons, and virtually none for non-U.S. persons.[47] Moreover, once the FISC approves those procedures, the NSA selects its surveillance targets in secret without any judicial review whatsoever.

22. What little oversight the FISC exercises is severely hampered by a near total lack of transparency about its proceedings and decisions. FISC proceedings are almost entirely secret, supposedly to preserve the integrity of covert surveillance operations. Until the Snowden revelations, only three opinions issued by the FISC and its appeals court, the Foreign Intelligence Surveillance Court of Review, had been published.[48] And for the most part, the FISC hears arguments only from the government as to whether a surveillance activity is permissible under the law. The lack of a transparent and adversarial process emboldened the government to advance and the court to endorse sweepingly broad interpretations of U.S. intelligence statutes to justify mass surveillance. One of the key orders withheld from the public until 2013 – and the first Snowden document that was published by the press – was an order from the FISC under Section 215 of the PATRIOT Act authorizing the collection of *all* records of telephone calls made to, from and within the U.S.[49] The plain text of Section 215 permits only collection of only those business records that are "relevant" to a terrorism or foreign intelligence investigation. The FISC's interpretation of the word "relevant," revealed in the subsequently released order justifying the program, effectively renders the concept of "relevance" utterly meaningless.[50]

23. The lack of a transparent and adversarial process in the FISC makes it virtually impossible for that court to meaningfully review large-scale surveillance operations. Unlike warrants that target specific individuals,[51] programmatic surveillance orders allow the government to sweep up the data and communications of millions of individuals at home and abroad with little or no regard for whether they are linked to suspected criminal or terrorist activity. The court's former presiding judge has admitted that the court is forced to rely on the intelligence agencies to report and correct noncompliance with the few statutory safeguards that exist.[52]

24. The FISC's reliance on U.S. intelligence agencies to self-regulate creates tremendous potential for abuse and wrongdoing. Indeed, even the limited number of court records and government documents that have been made public thus far reveal a litany of "noncompliance incidents." In March 2009, for example, the court found that the privacy safeguards it imposed on the government's telephone metadata program had "been so frequently and systematically violated that it can fairly be said that this critical element of the overall regime has never functioned effectively."[53] And in May 2012, an internal government audit recorded 2,776 violations of FISC-mandated privacy safeguards over a one-year period. These violations arose from the unauthorized collection, retention and distribution of information concerning Americans and foreign targets in the United States.[54]

V. Lack of An Effective Remedy for Privacy Violations

25. Because FISC proceedings are secret, persons affected in the United States usually do not know that they have been targeted by court-approved surveillance operations, and have little or no opportunity to challenge their surveillance. Although U.S. criminal defendants may be notified and are theoretically afforded a right to challenge the surveillance in some cases, this has ultimately proved illusory. If evidence derived from surveillance under FISA is used in a criminal prosecution, the law requires the government to notify the defendant of this fact and allow him or her to file a motion to suppress the evidence. In practice, however, the government has admitted that, until late 2013, its prosecutors failed to notify criminal defendants when evidence against them stemmed from warrantless surveillance under Section 702 of FISA.[55] In some cases, the government reportedly "recreated" the trail of evidence, effectively covering up the investigation's origin to circumvent the notification requirements.[56]

26. Although the government has recently begun to notify criminal defendants when it intends to use evidence derived from Section 702 against them, such notice is extremely limited. No defendant has ever been permitted to view the government's surveillance

applications, making it extremely difficult to challenge the scope and nature of their surveillance.

27. U.S. persons whom have not been charged with a crime but nevertheless have reason to believe they have been spied on encounter even greater difficulties in challenging the legality of the government's surveillance operations. In February 2013, the U.S. Supreme Court in *Clapper vs. Amnesty International* held that a group of lawyers, journalists and human rights activists lacked standing to challenge the government's alleged surveillance of their communications.[57] Plaintiffs had argued that given the nature of their work, it was likely that their communications were intercepted by the government. The Court rejected this argument, reasoning that since the plaintiffs had "no actual knowledge of the government's [surveillance] practices," allegations that their communications had been monitored were too speculative to allow them to sue.[58] Crucially, the Court also concluded that criminal defendants would have legal standing to trigger judicial review of the government's surveillance practices under FISA, relying on the government's assurances that it notified defendants appropriately.[59] As explained above, these assurances were false, and contributed to the Court's restrictive view of standing. Although Snowden's revelations have paved the way for several legal and constitutional challenges to NSA surveillance, the *Clapper* decision may thwart judicial review of surveillance programs that remain secret, or invasive programs that the government secretly introduces in the future.

28. As for non-U.S. persons located abroad, the possibility of judicial relief is even more illusory. In the event of a privacy violation involving a non-U.S. person, PPD-28 permits the Director of National Intelligence to notify the relevant foreign government in some cases.[60] However, it is unclear what substantive remedy the non-U.S. person might enjoy apart from notification of his government. The lack of an effective remedy stems partly from the fact that most electronic surveillance abroad takes place under Executive Order 12333, which is administered and regulated purely by the executive branch.

VI. Recent Reform Attempts

29. In the wake of Snowden's revelations, international human rights bodies have urged the U.S. to ensure that its surveillance laws and practices comply with the principles of legality, proportionality and necessity, "regardless of the nationality or location of the individuals whose communications are under direct surveillance."[61] However, neither of the government's two main reform efforts – Presidential Policy Directive 28 ("PPD-28") and the proposed FREEDOM Act – meaningfully limits the collection, use, retention and dissemination of communications and data linked to non-U.S. persons.

a. PPD-28

30. On January 17, 2014, President Obama released PPD-28 in response to growing criticisms of the U.S. government's surveillance practices.[62] The Directive recognized that U.S. signals intelligence activities "must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside." However, while the Directive is long on these "values" statements, a closer analysis of its provisions raises questions about the extent to which it reflects any changes in U.S. policy and practice. PPD-28 suffers from three principal shortfalls:

    i. *PPD-28 exempts a large number of surveillance programs from its 'use' restrictions*: PPD-28's restrictions on use of information acquired through surveillance apply only to programs that the government defines as "bulk collection." However, as explained above, the government's definition of "bulk collection" is extremely narrow and excludes many surveillance programs that sweep up massive amounts of communications and data without individualized suspicion of criminal or terrorist activity.[63]

    ii. *Failure to address bulk collection*: While PPD-28 restricts the *uses* of "signals intelligence collected in bulk," it fails to limit the scope of *collection*. The Directive merely reiterates the government's authority to collect communications for an extremely broad range of "foreign intelligence" and "counterintelligence" purposes,[64] including the authority to collect any information related the "capabilities, intentions and activities of foreign powers, organizations or persons."

    iii. *Failure to meaningfully restrict the sharing and dissemination of personal information belonging to non-U.S. persons*: PPD-28 extends restrictions on the sharing and dissemination of U.S. persons' information collected under EO 12333 to non-U.S. persons.[65] However, these restrictions are extremely permissive, and may be of even less value to non-U.S. persons. For example, EO 12333 allows the NSA to retain and share "information that constitutes foreign intelligence," which includes "information relating to the capabilities, intentions and activities of foreign … persons." Such a broad definition may effectively allow the NSA to retain and share a significant amount of information about non-U.S. persons that it could not retain and share about U.S. persons.

b. USA FREEDOM Act

31. While many bills have been introduced in the U.S. legislature to reform the NSA's surveillance practices, they fail to fully address the rights of non-U.S. persons. Even the bill that enjoys the most support among privacy and civil liberties groups – the USA FREEDOM Act, which was introduced by U.S. Senator Patrick Leahy and U.S. Representative Jim Sensenbrenner in October 2013 – does not sufficiently address the rights of non-Americans.[66] After extensive negotiations between Congress, and after President Obama's administration watered down the original version, the most recent iteration of the bill:

    i. *Prohibits the bulk collection of telephone and other records*: The Act would limit collection of metadata about telephone calls to, from and within the U.S. to cases where there is a "reasonable, articulable suspicion" that a "specific selection term" (SST) is associated with international terrorism.[67] For call detail records, the Act contains an exhaustive list of permissible SSTs. For other types of records, the Act prohibits the use of certain types of SSTs, such as cities, which are likely to return a large number of records.

    ii. *Requires additional minimization procedures*: In certain cases involving surveillance under Section 215 of the PATRIOT Act, the Act would mandate that the government adopt minimizations procedures requiring the destruction of information within a reasonable time frame. These procedures would apply in cases where the government does not make an affirmative determination that the information belongs to the target of an authorized investigation, or to an individual associated with or likely to have knowledge of the target.

    iii. *Introduces changes to the FISC:* The Act mitigates the lack of an adversarial process in the FISC by establishing a panel of special advocates to serve as *amici curiae*, or friends of the court. These advocates would provide input and argue in favor of civil liberties and the right to privacy, and would have access to relevant material. But the court has ultimate control over whether they would be allowed to appear or argue in cases that arise.

    iv. *Implements new transparency measures:* The Act would facilitate the declassification of "significant" FISC opinions, require the disclosure of certain statistics on the number of people whose data was collected, and permit the private sector to report figures on surveillance activities impacting users.

32. If passed, the USA FREEDOM Act would be a step in the right direction. But it has major gaps. It does not address Section 702 of FISA, which allows the government to intercept vast quantities of international communications available within the United States. It also does not address surveillance conducted under Executive Order 12333, under which an enormous amount of surveillance of both U.S. and non-U.S. persons alike occurs abroad.[68]

VII. Recommendations

33. **In light of the analysis above, we propose the following recommendations:**

i. **The U.S. should unambiguously recognize that it owes a duty under human rights law (particularly under Articles 2(1) and 17 of the ICCPR) to respect the privacy of individuals outside its territorial borders when it acquires, processes, analyzes, uses, retains or disseminates their digital communications and data.**

ii. **In the context of foreign intelligence gathering, the U.S. should acquire and monitor communications, personal information, metadata and other personal and sensitive data only when the information is necessary for the protection of specifically articulated U.S. national security interests, and only in a manner that produces the least intrusion on rights necessary to secure those interests.**

iii. **In the context of foreign intelligence gathering, the U.S. should adopt minimization procedures to ensure that information belonging to both U.S. and non-U.S. persons is used, retained and disseminated only when necessary for the protection of specifically articulated U.S. national security interests and in a manner that produces the least intrusion on rights necessary to secure those interests.**

iv. **With only those redactions that are truly necessary to protect legitimate national security interests, the U.S. should publish any court or executive order, opinion, directive, or document that contains significant legal interpretations of the U.S.'s surveillance laws and orders, especially Executive Order 12333.**

v. **The U.S. should reform current procedural laws (including but not limited to laws that regulate access to the FISC, FISC rules of procedure, notification**

requirements and the laws on standing) and establish appropriate remedial mechanisms to ensure that both U.S. and non-U.S. persons affected by U.S. foreign intelligence surveillance operations are capable of obtaining effective remedies for privacy violations arising from such operations.

---

[1] This submission does not purport to convey the position of NYU School of Law.

[2] Human Rights Council, Rep. of the Working Group on the Universal Periodic Review: United States of America, 16th Sess., §92.59, U.N. Doc. A/HRC/16/11; GAOR, 66th Sess., (Jan. 4, 2011) [hereinafter UPR-USA 2011], *available at* http://www.ushrnetwork.org/sites/ushrnetwork.org/files/working_group_report_upr_usa_2011.pdf.

[3] *Id*. at § 92.187.

[4] U.S. DEPT. OF STATE, U.S. RESPONSE TO UN HUMAN RIGHTS COUNCIL WORKING GROUP REPORT, ¶ 13, (2011), *available at* http://www.state.gov/j/drl/upr/archive/157986.htm .

[5] 50 U.S.C. §1861(a).

[6] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order .

[7] *See In re* Production of Tangible Things From [REDACTED], No. BR 08-13, slip op. at 4-11 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

[8] A press release from the Office of the Director of National Intelligence states that "In 2011, the Director of NSA called for an examination of this program to assess its continuing value as a unique source of foreign intelligence information. This examination revealed that the program was no longer meeting the operational expectations that NSA had for it." Press Release, Office of the Director of National Intelligence, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act, (Nov. 18, 2013) *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/964-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act-nov

[9] A non-U.S. person is a person that is not a "citizen of the United States" or "an alien lawfully admitted for permanent residence." *See* 50 U.S.C. § 1801(i).

[10] 50 U.S.C. §1881(a).

[11] *NSA Slides Explain the PRISM Data-Collection Process*, WASH. POST, June 6, 2013, [hereinafter *NSA Slides*] *available at* http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[12] According to prominent surveillance journalist James Bamford, the NSA relies on PRISM to fill in "gaps in [UPSTREAM's] coverage." James Bamford, *They Know Much More Than You Think*, THE N.Y. REVIEW OF BOOKS, Aug. 15, 2013, *available at* http://www.nybooks.com/articles/archives/2013/aug/15/nsa-they-know-much-more-you-think/?pagination=false; *See also* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 7, 2013, *available at* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

[13] These targets may not simply be individuals, and may refer to large groups such as "al-Qaeda" or "al-Shabab". *See NSA Slides, supra* note 11.

[14] *See* Ryan Devereux, Glenn Greenwald, & Laura Poitras, *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, THE INTERCEPT, May 19, 2014, *available at* https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas; Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, WASH. POST, Mar. 18, 2014, *available at* http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

[15] Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-Mail Address Books Globally*, WASH. POST, Oct. 14, 2013, [hereinafter *NSA Collects Millions*], *available at* http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

[16] Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, THE GUARDIAN [hereinafter *NSA Infiltrates Links*], Oct. 30, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[17] *Id.*

[18] Exec. Order No. 12,333, 3 C.F.R. 200 (1981).

[19] John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets The NSA Spy On Americans*, WASH. POST, Jul. 18, 2014, *available at* http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html; Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y TIMES, Aug. 13, 2014, *available at* http://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html.

[20] U.S. DEPT. OF STATE, FOURTH PERIODIC REPORT OF THE UNITED STATES OF AMERICA TO THE UNITED NATIONS COMMITTEE ON HUMAN RIGHTS CONCERNING THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS, §504-505 (2011), *available at* http://www.state.gov/j/drl/rls/179781.htm; U.S DEPT. OF STATE, UNITED STATES WRITTEN RESPONSES TO QUESTIONS FROM THE UNITED NATIONS HUMAN RIGHTS COMMITTEE CONCERNING THE FOURTH PERIODIC REPORT, § 2 (2013), *available at* http://www.state.gov/j/drl/rls/212393.htm.

[21] Human Rights Council, The Right to Privacy in the Digital Age: Rep. of the Office of the United Nations High Commissioner for Human Rights, ¶ 32, U.N. Doc. A/HRC/27/37; GAOR (June 30, 2014) [hereinafter OHCHR Report], *available at* http://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a.hrc.27.37_en.pdf; Human Rights Committee, CCPR General Comment No. 31[80]: The Nature of the General Legal Obligation Imposed on States Party to the Covenant, ¶ 10, (2004), *available at* http://www.refworld.org/docid/478b26ae2.html.

[22] OHCHR Report at ¶ 33, *supra* note 21.

[23] *See* Conor Friedersdorf, *Is the 'Five Eyes Alliance' Conspiring To Spy On You?* ATLANTIC (June 25, 2013), *available at* http://www.theatlantic.com/politics/archive/2013/06/is-the-five-eyes-alliance-conspiring-to-spy-on-you/277190/; Paul Farrell, *History of 5 Eyes- Explainer*, GUARDIAN, Dec. 2, 2013, *available at* http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

[24] Note, however, that a senior government official interviewed by the Human Rights Watch and the ACLU mentioned that there is a general principle reflected in EO 12333 that the U.S. government will not ask other governments to do what the U.S. cannot legally do (for example, monitor a U.S. person). Nevertheless, the official acknowledged that the U.S. government can accept information from other governments that it cannot legally collect on its own. G. ALEX SINHA, WITH LIBERTY TO MONITOR ALL, (HUMAN RIGHTS WATCH & AMERICAN CIVIL LIBERTIES UNION, 2014), *available at* http://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf.

[25] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies & James Ball, *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications,* GUARDIAN, Jun. 21, 2013, available at http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[26] James Ball, Julian Borger & Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN (Sept. 5, 2013), *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[27] Glenn Greenwald, Ewan MacAskill, & Laura Poitras, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, THE GUARDIAN (Sept. 11, 2013), *available at* http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

[28] A FISA court document states that, "Although admittedly a substantial portion of the telephony metadata that is collected would not relate to operatives of [REDACTED], the intelligence tool that the Government hopes to use to find [REDACTED] communications—metadata analysis—requires collecting and storing large volumes of the metadata to enable later analysis. All of the metadata collected is thus relevant, *because the success of this investigative tool depends on bulk collection*." (emphasis added) *Mem. Of Law In Support of Application For Certain Tangible Things For Investigations to Protect Against International Terrorism*, No. BR 06-05, at 15, (FISA Ct. [REDACTED]), *available at* https://www.aclu.org/files/assets/Production%20to%20Congress%20of%20a%20May%2023,%202006%20Government%20Memorandum%20of%20Law.pdf.

[29] DEPARTMENT OF DEFENSE, ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS, [HEREINAFTER ACTIVITIES OF DOD INTELLIGENCE COMPONENTS] § C.2.2.1.,DOD 5240 1-R, (1982), *available at* http://dtic.mil/whs/directives/corres/pdf/524001r.pdf.

[30] Human Rights Committee, CCPR General Comment No. 16: Article 17, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, ¶ 8-10 (1988), *available at* http://www1.umn.edu/humanrts/gencomm/hrcom16.htm.

[31] Amann v. Switzerland, 27798/95 Eur. Ct. H.R. (2000), ¶69, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58497#{"itemid":["001-58497"]}.

[32] OHCHR Report at ¶ 17-20, *supra* note 21.

[33] *Id.* at ¶ 21 - 23; Human Rights Council, Report of the Special Rapporteur on the Promotion And Protection Of Human Rights And Fundamental Freedoms While Countering Terrorism, Martin Scheinin. ¶ 16-19, U.N. Doc. A/HRC/13/37; GAOR (December 22, 2009); Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, ¶ 28-29, A/HRC/23/40; GAOR (April 17, 2013). *See also* ELECTRONIC FRONTIER FOUNDATION ET AL, 13 INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATION SURVEILLANCE (2ND ED.,2014) *available at* https://www.eff.org/document/13-international-principles-application-human-rights-communication-surveillance.

[34] Brett Max Kaufman, *A Guide to What We Now Know About the NSA's Dragnet Searches of Your Communications*, A.C.L.U., Aug. 9. 2013, *available at* https://www.aclu.org/blog/national-security/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications

[35] *NSA Infiltrates Links* supra note 16.

[36] Section 5 of PPD-28 excludes the practice of "temporarily" acquiring signals intelligence "to facilitate targeted collection." In other words, both the collection of "large quantities of signals intelligence data" with the "use of discriminants" at acquisition, as well as temporarily copying all communications in a vast communications stream and searching those communications against such discriminants, are considered "targeted collection." This overly broad definition of "targeted collection" would presumably shield many of the NSA's large-scale collection practices from the Directive's mandate to use information collected in "bulk" only for specific national security purposes. *See* Press Release, The White House, Office of the Press Sec'y, Presidential Policy Directive (PPD)- 28, at § 5 (Jan. 17, 2014) [hereinafter PPD-28], *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[37] Indeed, the NSA has asserted the authority under Section 702 of the amendments to FISA to "acquire communications about the target that are not to or from the target." *See* NATIONAL SECURITY AGENCY, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, 1 (2009), *available at* http://s3.documentcloud.org/documents/716633/exhibit-a.pdf.

[38] See ACTIVITIES OF DOD INTELLIGENCE COMPONENTS § C.3.3. *supra* note 29.

[39] *See* UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE, USSID SP0018 (U)LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZING PROCEDURES, 5.1., (NATIONAL SECURITY AGENCY, 2011), *available at* http://s3.documentcloud.org/documents/836235/ussid-sp0018.pdf; Section 5.1 of US Signals Intelligence Directive 18 permits the use of selection terms to "INTERCEPT a communication on the basis of the

content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMUNICANT or the fact that the communicant mentions a particular individual."

[40] 50 U.S.C. § 1801(e).

[41] Exec. Order No. 12,333, § 3.4(d), 3 C.F.R. 200 (1981 Comp.), *reprinted in* 50 U.S.C § 401 (Supp. V 1981).

[42] Smith v. Maryland, 442 U.S. 735 (1979).

[43] OHCHR Report, ¶ 19, *supra* note 21.

[44] Case C-293/12, Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, ¶ 19–22, 2014 E.C.R.

[45] Riley v. California, 134 S. Ct. 2473, 2490 (2014)

[46] United States v. Jones, 132 S. Ct. 945, 957 (2012), (Sotomayor J., concurring).

[47] 50 U.S.C. § 1881(a); 50 U.S.C. § 1881(d)(2); 50 U.S.C. § 1881(e)(2).

[48] *In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002); *In re* Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002); *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008).

[49] *See, e.g.*, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc., [hereinafter Order From Verizon], No. BR 13-80, at 1-2 (FISA Ct. July 19, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

[50] The Privacy and Civil Liberties Oversight Board (an independent agency within the executive branch of the government that advises the President and other senior officials on privacy and civil liberties concerns arising from the development and implementation of laws and policies related to counterterrorism) has stated that this interpretation of "relevance" is "untenable." *See* Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Act*, 60-81 (Jan. 23, 2014), *available at* http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program.pdf.

[51] The FISC also reviews applications for the electronic surveillance of specific targets that the government has probable cause to believe is a foreign power or an agent of a foreign power. *See* 50 U.S.C. § 1805(a)(2)(A).

[52] In response to the release of an internal audit showing the NSA had overstepped its legal authority thousands of times since 2008, former Presiding Judge Walton wrote in a statement to The Washington Post that "the FISC is forced to rely upon the accuracy of the information that is provided to the Court" and "does not have the capacity to investigate issues of noncompliance." *See* Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, WASH. POST, Aug. 15, 2013, *available at* http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html.

[53] *In re* Production of Tangible Things From [REDACTED], No. BR 08-13, at 11 (FISA Ct. Mar. 2, 2009), *available at* https://www.aclu.org/files/assets/pub_March%202%202009%20Order%20from%20FISC.pdf.

[54] Memorandum from Chief, SID Oversight and Compliance, to Director, SIGINT, NSAW SID Intelligence Oversight Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2013), ¶ 2 (May 3, 2012), *available at* http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/.

[55] Charlie Savage, *Door May Open For Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, *available at* http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?pagewanted=2&_r=0.

[56] John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used To Investigate Americans*, REUTERS, Aug. 5, 2013, available at http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 .

[57]133 S. Ct. 1138 (2013).

[58] *Id.* at 1141.

[59] Pet'r's Br. 15, 133 S. Ct. 1138 (2013) (No. 11-1025), *available at* http://www.americanbar.org/content/dam/aba/publications/supreme_court_preview/briefs/11-1025_pet_reply.authcheckdam.pdf.

[60] PPD-28, § 4(a)(iv), *supra* note 36.

[61]At the conclusion of the 2014 review of the U.S.'s compliance with the ICCPR, the Human Rights Committee recommended that the U.S. "[t]ake all necessary measures to ensure that its surveillance activities … compl[y] with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance." *See* Human Rights Committee, Concluding Observations on the Fourth Periodic Report of the United States of America, ¶ 22(a), U.N. Doc. CCPR/C/USA/CO/4,(April 23, 2014) *available at* http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en; Similarly, the OHCHR recommended that states, including the U.S. should review their national surveillance laws and practices "to ensure full conformity with international human rights law." *See* OHCHR Report at ¶ 50, *supra* note 21.

[62] PPD-28, *supra* note 36.

[63] *Id.*, fn. 5.

[64] *Id.*, § 1, fn. 2.

[65] *Id.*, § 4(a)(i).

[66] S. 1599, 113th Cong. (2014).

[67] The Act would limit the collection of these records under Section 215 of the PATRIOT Act, pen register and trap and trace authorities under FISA (*see* 50 U.S.C. §1842), and various National Security Letter authorities.

[68] *See Meet Executive Order 12333*; *Reagan-Era Order supra* note 19.