NSA Mass Surveillance Programs

Unnecessary and Disproportionate

David Greene, EFF Senior Staff Attorney
Katitza Rodriguez, EFF International Rights Director

This document was produced by the Electronic Frontier Foundation (EFF), an international non-governmental organization with nearly 30,000 members worldwide from over 100 countries, dedicated to the protection of everyone's right to privacy, freedom of expression, and association. Founded in 1990, EFF engages in strategic litigation, policy, and advocacy in the United States and works in a range of international and national policy venues to promote balanced laws that protect human rights, foster innovation, and empower consumers. EFF is based in San Francisco and was one of the key civil society groups involved in the drafting of the Necessary and Proportionate Guiding Principles.

Table of Contents

Foreword

The focus of this paper is to show how the publicly-known National Security Agency (NSA) surveillance operations constitute a violation of human rights as defined by international human rights norms. EFF supports the concluding recommendation of the 2014 Human Rights Committee[1] on the United States' compliance with the International Covenant on Civil and Political Rights (ICCPR), which calls upon the United States to take measures to ensure that any interference with the right to privacy comply with the principles of legality, proportionality, and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance.[2]

We have used the International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles" or "Thirteen Principles")[3] as a guiding framework to explain how the United States is currently failing to implement those existing human rights protections. The Principles have been endorsed by 400 organizations; they have also gathered support from European and Canadian Parliamentarians, political parties in several States,[4] and various prominent domain experts.[5] The Principles were developed to apply existing human rights law to the issues arising from the technically sophisticated and pervasive digital surveillance of ordinary individuals. This is, of course, most relevant to the c*ommunications surveillance*[6] being conducted by the NSA and GCHQ. But similarly intrusive practices are also achievable, and are likely currently practiced, by many States.

EFF believes that, in order to restore the strong protections provided for by international human rights law, we do not need a new human rights framework. Instead, we need to interpret and apply existing human rights protections appropriately in light of new technological developments and changing patterns of communications, and do so with an

1 The Human Rights Committee is the treaty body that monitors State implementation of the ICCPR, the main human rights treaty.

2 The Human Rights Committee's Concluding Observations during its 110th session. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=625&Lang=en

3 "International Principles on the Application of Human Rights to Communications Surveillance." Available in over thirty languages. July 10, 2013. https://necessaryandproportionate.org/text

4 https://necessaryandproportionate.org/text#elected_officials_political_parties

5 https://necessaryandproportionate.org/text#experts

6 According to the Principles, "Communications surveillance" in the modern environment encompasses the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, arises from or is about a person's communications in the past, present, or future. "Communications" include activities, interactions, and transactions transmitted through electronic media, such as content of communications, the identity of the parties to the communications, location-tracking information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.

intention to protect human rights. As with all human rights protections, we need to implement these steps in domestic laws to ensure everyone's right of privacy remains legally protected in the digital age.

Executive Summary

As set forth below, the US mass communications surveillance programs, as conducted by the NSA and exposed by Edward Snowden and other whistleblowers, violate several of the Necessary and Proportionate Principles:

- The NSA surveillance lacks "**legality**" in that NSA surveillance laws are largely governed by a body of secret law developed by a secret court, the Foreign Intelligence Surveillance Court (FISC), which selectively publishes its legal interpretations of the law;
- The NSA surveillance programs are neither "**necessary**," nor "**proportionate**," in that the various programs in which communications data are obtained in bulk violate the privacy rights of millions of persons who are not suspected of having any connection to international terrorism;
- The NSA surveillance programs are not supported by **competent judicial authority** because the only judicial approval, if any, comes from the secret Foreign Intelligence Surveillance Court, and access to courts is largely denied to the individuals whose data are collected;
- The NSA surveillance programs lack **due process** because there is frequently no opportunity for a public hearing;
- The NSA surveillance programs lack **user notification**; those whose data is obtained do not know that their communications have been monitored and therefore cannot appeal the decision nor acquire legal representation to defend themselves;
- The NSA surveillance programs operate in secret and thus rely on gag orders against the entities from whom the data is obtained. The secret court proceedings, if there are any, lack necessary **transparency** and **public oversight**;
- The NSA surveillance programs damage the **integrity of communication systems** by undermining security systems (such as encryption), requiring the insertion of surveillance back doors in communications technologies, including the installation of fiber optic splitters in transmission hubs; and
- The US surveillance framework is illegitimate because it applies less favorable standards to non-US persons than its own citizens; this **discrimination** places it in violation of the International Covenant on Civil and Political Rights (ICCPR) as well.

Moreover, the United States justifies the lawfulness of its communications surveillance by reference to distinctions that, considering modern communications technology, are

solely semantic rather than substantive. The US relies on the outmoded distinction between "content" and "metadata," falsely contending that the latter does not reveal private facts about an individual. The US also contends that the collection of data is not surveillance—it argues, contrary to both international law and the Necessary and Proportionate Principles, that an individual's privacy rights are not infringed as long as her communications data are not analyzed by a human being.

A Brief Survey of Ongoing NSA Surveillance Activities

NSA surveillance takes place in a framework of massive secrecy. It is easy to view those programs and activities,whose existence has been revealed in the press over the course of the past year, as the primary or representative activities of the intelligence agencies. And, indeed, much political commentary has focused on the most widely-documented of the programs, such as the collection of telephone calling records from US carriers. But the full extent of these programs, and the percentage of total US governmental surveillance they comprise, remains unknown. The operations described in this paper, then, represent only a very small selection of the overall pervasive surveillance activities carried out by NSA and other intelligence agencies—and even that view is limited in terms of the details it conveys regarding the scope and content of each such operation. Some operations, for example, may actually be software analysis tools for performing particular kinds of searches or analysis over data that has already been acquired by some other means. In this scenario, "surveillance programs" may not always involve gathering any new data or obtaining any new access to devices, networks, or signals; they might just involve interpreting data that NSA or other intelligence agencies *already have access to* or *already have in their databases*, and drawing new inferences from those records or combining them to reach new conclusions.[7]

This scenario makes clear that a core privacy interference occurs when States first acquire, monitor, and/or collect information about people, even if the purpose of such collection was highly general and did not contemplate specific intrusions.

Origins of the Current Programs

Following the terrorist attacks against the US on September 11, 2001, President George W. Bush empowered the NSA and other components of the US intelligence community to conduct wide-ranging surveillance without court orders or oversight. The surveillance was collectively called the President's Surveillance Program (PSP). The PSP remained a secret until 2005 when the existence of small parts of it were revealed by newspaper

7 A great deal of information about people, places, devices, and electronic communications seems to lack privacy sensitivity when taken in isolation, but when combined with other data may turn out to be extremely significant and sensitive. For instance, an individual telephone call takes on a new significance when we learn that the called party was a specialist medical clinic or a hotline for particular medical, psychiatric, abuse, or financial problems. Individual records of logins to an Internet service take on new significance when multiple users' records are read together to infer that those users did or did not spend the night in the same place.

reports.[8] Between 2004 and 2007, the US government moved many of the PSP projects under the authority of the Foreign Intelligence Surveillance Court, via various legal interpretations, and this continued with the passage of the FISA Amendments Act in 2008. This, for the first time, exposed those actions to any level of judicial review.[9]

However, some of the current surveillance activities continue to operate without judicial authorization. As discussed below, activities aimed at non-US communications can operate under the purported authority of Executive Order 12333 and are styled as executive acts not subjected to judicial approval or review. It is also not clear which of these programs were in operation prior to the September 11 attacks. Attempts to use technical means to gain access to massive amounts of private communications data are not new. It is known that the NSA conducted some form of broad surveillance prior to the attacks, for example, through the ECHELON program.[10]

Known Ongoing Mass Surveillance Activities

The NSA is known to engage in the following forms of mass surveillance of communications, organized according to the purported legal authority for each program. In addition to raising human rights concerns for US persons, an overarching issue, especially for the international community, is that for each program noted below, the US government takes the position that any protections against surveillance, such as the "minimization" steps taken after the collection, are aimed at protecting the rights of US persons only, whose information may be collected as a by-product of the collection of information from non-US persons. Historically, the United States has asserted no legal protection for the privacy rights of non-US persons outside of the United States and has not recognized any normative limits on the US government's ability to monitor these communications to any extent and for any reasons and this position should be soundly rejected.

FISA Section 702 (50 U.S.C. sec. 1881a)

Section 702 was added to the FISA by the FISA Amendments Act in 2008. The US has asserted that Section 702 authorizes the collection of communications of "non-US persons" inside the United States for foreign intelligence purposes, and that it, in its

8 Following these disclosures, the administration of President George W. Bush acknowledged the existence of some of these disclosed PSP activities, collectively labeling them the "Terrorist Surveillance Program" or TSP. But the term TSP appears to have no operational definition or significance.

9 The Foreign Intelligence Surveillance Act of 1978 put into place procedures for the surveillance of foreign intelligence information. Among those procedures was the creation of the Foreign Intelligence Surveillance Court (FISC). The FISC was created to provide some level of judicial oversight of specific instances of surveillance when conducted inside the US, through approval of individual warrants. Although the FISC is staffed by federal judges, it operates very differently from a federal district court. The proceedings of the FISC are secret and non-adversarial. The FISC has found that it has no obligation to publish its opinions, although it does exercise its discretion to publish its opinions when it so desires. In 2008, Congress passed the FISA Amendments Act, which greatly expanded the charge of the FISC, including granting it the ability to approve general procedures for surveillance, rather than merely approving a specific investigation or individual warrant.

10 European Parliament: Temporary Committee on the ECHELON Interception System—Rapporteur Gerhard Schmid. "On the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))." http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN. 11 July 2001.

efforts to collect the communications of non-US persons, may incidentally collect the communications of US persons as well. The NSA has also asserted that this mass collection of US and non-US persons' communications data is consistent with Section 702 because it only "targets" the materials pertaining to non-US persons. The US government considers a "target" a "non-US person" if it is more likely than not that the person is not a "US person." (A "US person" is defined as a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association with a substantial number of members who are citizens or lawful aliens, or a corporation incorporated in the United States).

The FISC must approve general targeting and minimization procedures—for example, any search terms used to query the collected data—but it does not review actual targets. These minimization procedures are designed primarily to protect US persons. The FISC review is ex parte, that is, conducted without the presence of an adversary, and the approved surveillance is never made public. Just recently, in response to concerns raised by the Supreme Court, the government has begun selectively notifying individuals who are facing criminal prosecution that information collected under the 702 program has been used in investigating them.[11]

The following operations are only a small subset of those publicly-known and operated under the purported authority of Section 702:

"Upstream"

- "Upstream" operations involve the installation of fiber optic splitters at numerous sites operated by private telecommunications companies throughout the US. The splitter provides the NSA with a complete copy of all Internet traffic (including communications content such as emails, search and browsing records, and VoIP communications) that passes through the installations.

PRISM

- PRISM was launched in 2007 as a means of collecting stored Internet communications data—such as email, video and video chat, photos, VOIP, file transfers, and social networking interactions—on demand from the servers of Internet companies such as Google, Microsoft, Apple, and Yahoo!.

USA PATRIOT Act Section 215

Section 215, also known as the "business records" provision, was enacted as part of the USA PATRIOT Act in 2001, and then amended in 2008 by the FISA Amendments Act. The law authorizes the FISC to issue orders permitting the FBI to collect "tangible things" that are "relevant to an authorized investigation," as might be obtained via a grand jury

11 "Udall, Wyden, Heinrich Urge Solicitor General to Set Record Straight on Misrepresentations to U.S. Supreme Court in Clapper v. Amnesty." http://www.wyden.senate.gov/news/press-releases/udall-wyden-heinrich-urge-solicitor-general-to-set-record-straight-on-misrepresentations-to-us-supreme-court-in-clapper-v-amnesty

subpoena. Section 215 orders cannot be directed at US persons solely on the basis of activities protected by the First Amendment.

The following are a small subset of publicly-known programs operated under the purported authority of Section 215:

CALL DETAIL RECORDS COLLECTION

- The US government, through the NSA, is collecting the call detail records from certain telephone service providers of every domestic and international telephone call made to or from their networks. The data collected include the telephone numbers on each end of the call, the time and length of the call, and the routing information. It is unclear whether specific location data is also collected under this program or under some other program. The content of the calls is not collected (which is why the US labels this data "metadata"). The records are retained for five years.
- The program is subject to re-approval by the FISC every 90 days. The database is queried by way of "selectors," such as telephone numbers, for which there is a "reasonable articulable suspicion" of a link to terrorism. The database is queried to identify every call made to or from the selector, and then as a second "hop," every call made to or from those numbers. Prior to January 2014, the analysis was carried out to a third "hop" as well. Several hundred selectors have been used since the beginning of the program that have resulted in the "selection" and further analysis of an unknown number of calls, but likely well into the millions.

Executive Order (EO) 12333

- Executive Order 12333 authorizes surveillance conducted primarily outside the United States, although there are indications that the government maintains that some amount of US-based surveillance can also occur under this authority.[12] President Ronald Reagan issued EO 12333 in December 1981 to extend the powers and responsibilities of the various US intelligence agencies that existed under previous executive orders. The organizational structure established by EO 12333 was revised by executive orders in 2004 and 2008, the latter of which consolidated power under the President's Director of National Intelligence. The US government asserts that programs conducted under the authority of EO 12333 do not require judicial approval or non-executive oversight of any type.[13]

The following is a small subset of publicly-known activities operated under the purported authority of EO 12333:

---

12 Executive Order (EO) 12333 was amended on January 23, 2003 by Executive Order 13284, on August 27, 2004 by Executive Order 13355, and further amended on July 30, 2008 by Executive Order 13470. The resulting text of Executive Order 12333, following the 2008 amendment, is available here http://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf

13 http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_print.html

MYSTIC

- Under this operation, the NSA has built a surveillance system capable of recording "100 percent" of a foreign country's telephone calls, enabling the agency to rewind and review conversations as long as a month after they take place,.[14] MYSTIC has been used against one nation, according recent leaks, and may have been subsequently used in other countries ..

MUSCULAR

- This operation, which began in 2009, infiltrates links between global data centers of technology companies, such as Google and Yahoo!, not on US soil. These two companies responded to the revelation of MUSCULAR by encrypting those exchanges.

XKEYSCORE

- XKEYSCORE appears to be the name of the software interface through which NSA analysts search vast databases of information—collected under various other operations—containing emails, online chats, and the browsing histories of millions of individuals anywhere in the world. The XKEYSCORE data has been shared with other secret services including Australia's Defence Signals Directorate and New Zealand's Government Communications Security Bureau.

BULLRUN

- Not in and of itself a surveillance program, BULLRUN is an operation by which the NSA undermines the security tools relied upon by users, targets and non-targets, and US persons and non-US persons alike. The specific activities include dramatic and unprecedented efforts to attack security tools, including:
    - Inserting vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets;
    - Actively engaging US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs;
    - Shaping the worldwide commercial cryptography marketplace to make it more vulnerable to the NSA's surveillance capabilities;
    - Secretly inserting design changes in systems to make them more vulnerable to NSA surveillance, and
    - Influencing policies, international standards, and specifications for commercial public key technologies.

---

14 Gellman, Barton and Ashkan Soltani. "NSA surveillance program reaches 'into the past' to retrieve, replay phone calls." 28 March 2014. 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

DISHFIRE

- The Dishfire operation is the worldwide mass collection of records including location data, contact retrievals, credit card details, missed call alerts, roaming alerts (which indicate border crossings), electronic business cards, credit card payment notifications, travel itinerary alerts, meeting information, text messages, and more. Communications from US phones were allegedly minimized, although not necessarily purged, from this database. The messages and associated data from non-US persons were retained and analyzed.

CO-TRAVELER

- Under this operation, the US collects location information from global cell tower, Wi-Fi, and GPS hubs. This information is collected and analyzed over time, in part, in order to determine the traveling companions of targets.

In addition to these programs, the NSA also surveilled messaging conducted through "leaky" mobile applications, monitored the mobile phone communications of 35 world leaders, and monitored, for example, approximately 70 million phone calls per month originating in France and 60 million per month originating in Spain. Also, the NSA collected financial records—180 million in 2011—from SWIFT, the network used by worldwide financial institutions to securely transmit interbank messages and transactions.

US Legal Challenges to NSA Surveillance

The US Government has asserted that its current communications spying operations are fully in compliance with international law, primarily by claiming that its practices are conducted according to domestic US law. However, there are several ongoing legal challenges in US courts to NSA surveillance, including several in which EFF serves as counsel.[15] These lawsuits challenge the programs as being both unconstitutional—under the 4th Amendment, 1st Amendment, and in some places the 5th Amendment of the United States Constitution—and illegal under the statutes used to justify them.

There have thus far been no legal challenges in US courts to any of the US actions under the purported authority of EO 12333 and no challenges directly regarding the rights of non-US persons.

Challenges to "Upstream" Internet Surveillance

The following lawsuits are challenges to the collection of Internet data through the installation of fiber optic splitters at transmission hubs:

15 EFF's statements and positions here are not those of its clients in the litigations where EFF is counsel and nothing said here shall be construed as a statement or admission by any of those plaintiffs.

- *Jewel v. NSA* (an action by AT&T customers in a federal court in California);[16]
- *Shubert v. Obama* (a class action on behalf of all Americans against the NSA's domestic dragnet surveillance);
- Criminal prosecutions: Section 702 surveillance is being challenged in several cases in which the government has brought criminal charges, largely terrorism-related. The defendants, many of whom only recently received notice of their prosecution despite being charged long ago, are mounting challenges to the evidence used against them on the grounds that it was illegally and unconstitutionally collected and used.

Challenges to Section 215 Telephone Call Detail Records Collection

The following lawsuits challenge the mass collection of telephone call detail records from US persons:

- *First Unitarian Church of Los Angeles v. NSA* (an action by 22 organizations in a federal court in California);[17]
- *Jewel v. NSA* (see above);
- *ACLU v. Clapper* (an action by the ACLU and its New York chapter in a federal court in New York; the trial judge dismissed the lawsuit, that dismissal is currently on appeal);
- *Klayman v. United States* (a class action in the federal court in the District of Columbia; the trial judge found the call detail records surveillance unconstitutional on 4th Amendment grounds; that decision has been appealed);
- *Smith v. Obama* (an action by an individual filed in a federal court in Idaho);
- *Paul v. Obama* (a class action filed in federal court in the District of Columbia);
- *Perez v. Clapper* (an action by two individuals filed in a federal court in Texas).

These lawsuits all address the legality of the program with respect to US persons. These lawsuits do not raise the non-discrimination rights of non-US persons under the ICCPR and European law, or the Inter-American system.

16 Jewel vs. NSA, https://www.eff.org/cases/jewel

17 First Unitarian Church of Los Angeles v. NSA, https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa

Application of the Principles to US Surveillance

The US surveillance programs plainly violate international human rights law, especially when compared to the Necessary and Proportionate Principles; the gaps between US surveillance programs and the standards for human rights are readily apparent.

The Necessary and Proportionate Principles are based upon the existence of a fundamental human right—the right to privacy—as recognized under international human rights law.[18] The right to privacy is not only a fundamental right in and of itself, it bolsters other fundamental rights as well—including freedom of expression, freedom of information, and freedom of association.[19]

Definitions

"Metadata"/"Content" Distinction

The Principles define "protected information" to include "all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public." The definition is aimed at protecting both privacy and freedom of expression, which in many cases flourishes only with assurances that communications and associations can remain free from governmental tracking. The Principles recognize that individuals, who believe that the government is gaining access to records containing information that reveals, for example, to whom they are speaking, when they are speaking, and for how long, especially over time, they are speaking, will be less willing to communicate about sensitive or political topics.

In doing so, the Principles expressly recognize that the old distinctions between content and "non-content" or "metadata" are "no longer appropriate for measuring the degree of intrusion that communications surveillance makes into individuals' private lives and associations." Indeed, "metadata" is information-rich; this information may reveal a person's identity, behavior, political and social associations, medical conditions, race, or sexual orientation. The information may enable the mapping of an individual's movements and interactions over time, revealing whether the individual was present at a

18 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

19 The freedom of association and freedom of speech are inherently linked. The freedom of association recognizes that individuals may have a stronger and more influential voice in public discussions by joining with other like-minded persons and advocating as a group. The right to privacy bolsters this right by allowing such groups to form and communicate while permitting the individual associates to remain anonymous. This ability to remain anonymous is especially important where the group's views are unpopular, dissenting, or involve deeply personal private information—situations in which one might choose not to speak at all if the fact of her association with the group were to become known.

political demonstration, for example. Because of this, the President's Review Group cited the Principles in noting that the distinction between content and non-content was increasingly untenable.[20]

Useful explanations about how using metadata can reveal intimate and private information about people are contained in a declaration—filed by Princeton professor, Edward Felten—in support of one of the lawsuits challenging the telephone records collection and recent research by a team from Stanford University, which notes how intimate details of a persons' life can be discerned from a relatively small amount of metadata.[21]

The Principles also instruct that "[w]hen adopting a new communications surveillance technique or expanding the scope of an existing technique, the State should ascertain whether the information likely to be procured falls within the ambit of 'protected information' before seeking it, and should submit to the scrutiny of the judiciary or other democratic oversight mechanism."

The US, particularly in justifying the Section 215 mass collection of call detail records, has relied on this distinction between "content" and "metadata," citing Supreme Court authority from over 40 years ago.[22] The US has argued that there are no privacy interests in non-content information protected by the 4th Amendment. This position is inconsistent with the Principles and inconsistent with the need to protect privacy and freedom of expression in the digital age.

Metadata Matters

IP addresses collected by a web service can reveal whether two people spent the night in the same place.

- This is because an IP address at a particular point in time will usually be unique to a single residence.
- If two people both logged in to services from the same IP address late at night and early in the morning, they probably spent the night together in the place distinguished by that IP address.

Stanford researchers found (experimentally) that information about who people call can be used to infer extraordinarily sensitive facts about them, including the fact that they sought and received treatment for particular a medical condition, that they had an abortion, or that they purchased firearms, among other things.[23]

---

20 "Liberty and Security in a Changing World; Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies." 12 Dec. 2013. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

21 Felton, Edward W. "Case 1:13-cv-03994-WHP Document 27," filed August 26, 2013. https://www.documentcloud.org/documents/781486-declaration-felten.html

22 Smith v. Maryland, 442 U.S. 735 (1979). http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&invol=735&vol=442

23 Mayer, Jonathan and Patrick Mutchler. "MetaPhone: The Sensitivity of Telephone Metadata." 12 March 2014. http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

Retail stores now have the ability to track individuals' physical whereabouts by observing data packets transmitted from smartphones and other mobile devices.

- They can recognize when people return to a store (and how often), see which part of the store visitors spend their time in, and figure out how long people wait in lines.
- Some entities are in a position to associate this information with a person's name because the entities observe mobile device identifiers together with other identifying information.

Law enforcement and intelligence agencies are using technology to track individuals' whereabouts—on a massive scale, twenty-four hours a day—whether by directly observing the signals transmitted from phones or by demanding that mobile carriers turn over information about users' locations.

- Information about where people go reveals sensitive religious, medical, sexual, and political information about them, including the kinds of medical specialists, religious services, or political meetings a person meets with or attends.
- Information about the proximity or lack of proximity of multiple people to one another can reveal individuals who attended a protest, the beginning or end of a romantic relationship, or a person's marital infidelity.
- Information from telephone companies has been repeatedly sought and used to identify the sources who gave information to journalists.

First Look Media's publication, *The Intercept*, reported that the United States is using telecommunications metadata as a means of targeting lethal drone strikes aimed at the cellular phones of individual people, recognized by wireless signals that they transmit.

In the Ukraine, cell tower dumps were used to determine who had participated in the Maidan protests against the previous regime, and then to let them know that the government was watching.

- The ability to automatically get a complete list of who attended a protest is an extremely serious threat to the freedom of expression and association if people believe that there is a potential for future backlash (or violence!) from being identified as a participant.

Bulk and Persistent Surveillance

According to the Principles, in determining whether surveillance will sweep up "protected information," the form, scope, and duration of the surveillance must be considered: "Because pervasive or systematic monitoring has the capacity to reveal private information far in excess of its constituent parts, it can elevate surveillance of non-protected information to a level of invasiveness that demands strong protection."[24]

24 "Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past…In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention." (Rotaru v. Romania, [2000] ECHR 28341/95, paras. 43-44).

The Section 215 program and significant kinds of collection under Section 702 and EO 12333 involve bulk or mass collection of communications data over an extended period of time on a continuous or nearly continuous basis. For the Section 215 program, at any point in time, the NSA is likely to have five years worth of call detail records about an individual.

"Collection" = "Surveillance" = Interference with Privacy

Much of the expansive NSA surveillance revealed in the past year has been defended by the United States on the basis that the mere collection of communications data, even in troves, is not "surveillance" because a human eye never looks at it. Indeed, under this definition, the NSA also does not surveil a person's data by subjecting it to computerized analysis, again up until the point a human being lays eyes on it. The Principles, reflecting the human right to privacy, defines "surveillance" to include the monitoring, interception, collection, analysis, use, preservation, and retention of, interference with, or access to information that includes, reflects, or arises from or a person's communications in the past, present, or future. States should not be able to bypass privacy protections on the basis of arbitrary definitions.

Applying the Principles

The Legality Principle

The first of the Necessary and Proportionate Principles is "Legality." Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly reviewable legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.

As the European Court of Human Rights has explained, "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[25] Thus the Legality principle requires that laws be non-secret and subject to oversight and that they not vest governmental officials with excessive discretion.[26]

---

25 Judgment in The Sunday Times v. The United Kingdom, Application no. 6538/74, Judgment of 26 April 1979, para.49.

26 Siver v. the UK, Petra v. Romania, 1998. The Human Rights Committee takes the very same approach. General Comment No. 34, CCPR/C/GC/34, 12 September 2011, paras. 24 – 26. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f34&Lang=en

The Legality principle is not a mere reference to domestic law. It is therefore not sufficient for the US to contend that its surveillance programs are sanctioned by US laws (even if that lawfulness were not subject to ongoing litigation).

The Legality principle is violated by the fact that the US surveillance programs are almost all conducted in secret, and are largely governed by a body of secret law developed by a secret court—the FISC—which selectively publishes its legal interpretations of the law. Many, if not most, of the FISC's rulings are not subject to public review or oversight; individuals are thus uninformed as to what their rights are vis-à-vis the US surveillance programs. Moreover, many of the programs, especially under EO 12333 as described above, are not subject to any judicial oversight, and lack any defined standards of implementation. This position has been recently confirmed by the UN Human Rights Committee in its concluding observations from the United States' review on its compliance with the ICCPR.

Necessity and Proportionality in Pursuit of a Legitimate Aim

The principle of "Necessity" reflects the requirement under International law that restrictions on fundamental rights, such as the right of privacy, must be strictly and demonstrably necessary to achieve a legitimate aim.

Each of these factors—necessity, legitimate aim, adequacy, and proportionality—is included in the Principles. As stated in the Principles, the State must establish "that (1) other available less invasive investigative techniques have been considered, (2) information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual, and (3) information is accessed only by the specified authority and used for the purpose for which the authorization was given."

The US mass surveillance programs under Section 215 and 702 and EO 12333 fail to meet these requirements in that the dragnet collection of information about non-suspicious individuals is a far too inclusive, and thus disproportionate, method. The US government is accumulating a tremendous amount of data and, as the US concedes, the vast amount of it will ultimately prove to be wholly unrelated to international terrorism. Moreover, the US legal system fails to require a threshold of showing for collection of any communications or communications records or an individualized suspicion for targeting non-US persons.

As Martin Scheinin, the former United Nations special rapporteur on human rights and counterterrorism, has noted, mass surveillance is inherently a disproportionate measure.[27] The collection of all data is seldom, perhaps never, a "necessary" measure, by

27 Joergensen, Rikke Frank. "Can human rights law bend mass surveillance?" 27 Feb. 2014. http://policyreview.info/articles/analysis/can-human-rights-law-bend-mass-surveillance

any definition of the word "necessary." Mass surveillance will inevitably and unavoidably sweep up masses of private information that will be of no use or relevance in anti-terrorism investigations.

This lack of necessity has been borne out, at least as to the Section 215 surveillance programs, by the reports of two committees, hand-picked by the President, the President's Review Group, and the Privacy and Civil Liberties Oversight Board. Each received classified information about the necessity and efficacy of the program and each concluded that it had not resulted in the prevention of any terrorist attacks or had even been more than marginally useful in a terrorism investigation.

Facts:

The US is "sitting on the wire," that is, much of the global Internet traffic travels through wires on US territory. The NSA accesses this traffic to illegitimately track who visits online pornography websites, and use this information to discredit those it deems dangerous.[28]
The FISA surveillance law was originally intended to be used only in certain specific, authorized national security investigations. But information-sharing rules implemented after 9/11 allow the NSA to hand over information to traditional domestic law-enforcement agencies, without any connection to terrorism or national security investigations.[29]
As the NSA scoops up phone records and other forms of electronic evidence while investigating national security and terrorism leads, they have turned over "tips" to a division of the Drug Enforcement Agency, which is inappropriate to fulfill the specific Legitimate Aim identified.[30]
The telephone records program, at least, has now been evaluated by two hand-picked Presidential panels to be *unnecessary*, since it has not had a significant impact in preventing terrorist attacks or been more than marginally useful to terrorism investigations in the United States.[31]

Competent Judicial Authority

The Principles require that "determinations related to communications surveillance must be made by competent judicial authority that is impartial and independent. This judicial authority must be: 1) separate from the authorities conducting communications surveillance; 2) conversant in issues related to and competent to make judicial decisions

28 Opsahl, Kurt. "The NSA is Tracking Online Porn Viewing to Discredit 'Radicalizers.'" 27 Nov. 2013. https://www.eff.org/deeplinks/2013/11/nsa-tracking-online-porn-viewing-discredit-radicalizers

29 Fakhoury, Hanni. "DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations." 6 Aug. 2013. https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering

30 *Id.*

31 Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. 12 Dec. 2013. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf See EFF's "Statement on President's Review Group's NSA Report." 18 Dec. 2013. https://www.eff.org/deeplinks/2013/12/eff-statement-presidents-review-groups-nsa-report See "President's Review Group Puzzler: Why is Massively Overbroad Surveillance Wrong under 215 but OK under Section 702?." 10 Jan. 2014. https://www.eff.org/deeplinks/2014/01/presidents-review-group-puzzler-why-mass-surveillance-wrong-under-215-ok-under

about the legality of communications surveillance, the technologies used and human rights; and 3) have adequate resources in exercising the functions assigned to them."

Significant doubts exist as to whether the mass surveillance operations are reviewed by "competent" judicial authority. With regard to surveillance under Patriot Act section 215 or FISA Amendments Act section 702, there are serious questions about whether the FISC has a sufficient understanding of the technologies used, or has sufficient resources to conduct the oversight required of it. The Chief Judge of the FISC, Judge Walton, has recognized that the court is limited in its ability to scrutinize the NSA's abuses: "The FISC is forced to rely upon the accuracy of the information that is provided to the Court…The FISC does not have the capacity to investigate issues of noncompliance."[32]

And as discussed above, there is no judicial oversight at all for NSA surveillance justified under under EO 12333.

Facts:

EO 12333 programs, consisting mainly of foreign collection, are conducted without any judicial involvement.[33]
Oversight of domestic collection programs is conducted by a secret court, the Foreign Intelligence Surveillance Court. The FISC is fully dependent on the authorities conducting the surveillance to provide it with information about their activities.

Due Process

The Principles require that every individual seeking a determination about whether or not her human rights are being infringed upon have access to "a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law."

NSA surveillance violates this principle in that those whose information is gathered are given neither notice nor any opportunity to contest the practice. The FISA and the FISA Amendments Act specifically limit judicial access to the FISC to the third-party entities from which the information is sought. Those about whom the information pertains have no opportunity to contest the demand made to the third party. Moreover, the US has stated that no telecommunication service provider who has been required to produce records under Sections 215 or 702 has ever contested those demands in the FISC. As a result, the FISC proceedings have been non-adversarial within a traditionally adversarial

32 Leonnig, Carol D. "Court: Ability to police U.S. spying program limited." 15 Aug. 2013. http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html.

33 Jaycox, Mark M. "Three Leaks, Three Weeks, and What We've Learned About the US Government's Other Spying Authority: Executive Order 12333." 5 Nov. 2013. https://www.eff.org/deeplinks/2013/10/three-leaks-three-weeks-and-what-weve-learned-about-governments-other-spying

judicial system—with the government presenting its case, but with no one representing the case against such surveillance practices.

While the litigation described above is attempting to bring at least some process to bear on the surveillance, the US government's position is that all such challenges should be dismissed without a substantive review of its activities.

Facts:

NSA surveillance violates due process since, at least as the government currently maintains, those subject to it have no right to learn about it, much less challenge it.
The New York Times reports that communications between an American law firm and its foreign client may have been among the information the Australian Signals Directorate shared with the NSA. Surveillance of attorney-client communications is anathema to the fundamental system of justice.[34]

User Notification

The Principles, with certain exceptions, require that individuals be notified of decisions authorizing surveillance of their communications with enough time and information to appeal the decision or seek other forms of remedial relief. However, with few exceptions, the Section 215 and 702 programs are conducted in secret and individuals are never notified that the NSA is collecting their communications data. Surveillance under EO 12333 is similarly conducted without notice. Moreover, those telecommunications service providers that do receive demands for business records, under Section 215, or any materials as described in National Security Letters, are forbidden from notifying anyone of the demands. These gags are perpetual.

Facts:

NSA surveillance prevents those surveilled to be notified about it, much less be notified in time to either challenge it beforehand or seek some remedial relief afterwards. The purported governing legal authority fails to require the NSA to provide notice, and requires that permanent gag orders be placed on service providers who were ordered to disclose their customers' data.

Transparency and Public Oversight

The Principles require that States be transparent about their use and scope of communications surveillance techniques and powers, and that they publish enough information to enable the public "to fully comprehend the scope, nature and application of the laws permitting communication surveillance." Service providers must be able to

34 Kayyali, Nadia. "The Tepid NSA-American Bar Association "Dialogue" Around Spying on Lawyers." 21 March 2014. https://www.eff.org/deeplinks/2014/03/tepid-nsa-american-bar-association-dialogue-around-spying-lawyers

publish the procedures they apply when addressing surveillance, adhere to those procedures, and publish records of surveillance.

The Principles further require that, "States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance." The Principles require independent oversight mechanisms in addition to any oversight provided through another branch of the government.

NSA surveillance does not meet these requirements. The NSA surveillance programs operate almost entirely in secret. Indeed, much of what we know now about the programs was provided to the public by various whistleblowers. The US government, until very recently, has steadfastly worked to make sure that the public does not "fully comprehend the scope, nature and application of the laws permitting communications surveillance." Moreover, service providers receiving demands for customer information are typically gagged from reporting even the fact of the demand.

First, many of the NSA surveillance programs are subject to no external oversight at all, such as those under EO 12333.

Second, even the programs subject to Congressional and judicial review face problems with transparency and accountability.[35] Although the programs run under the FISA are subject to FISC review—which has not been completely toothless; the FISC shut down the phone records collection for 9 months in 2009 because of the government's failure to comply with minimization procedures—there is no oversight provided by an external entity, as required by the Principles. Moreover, because it lacks technical expertise in anti-terrorism, the FISC is often forced to defer to the judgments made by the NSA regarding the effectiveness and necessity of the surveillance operations. The Senate Intelligence Committee, which provides Congressional oversight of the NSA, relies on the information provided by the NSA. Many members of Congress have complained of a lack of candor and a failure to provide sufficient information to allow them to conduct genuine oversight.[36]

Facts:

> Members of US Congress confirm that they were repeatedly misled about the mass surveillance or denied reasonable access to information necessary to conduct oversight.[37]

---

35 Cohn, Cindy and Mark M. Jaycox. "NSA Spying: The Three Pillars of Government Trust Have Fallen." 15 Aug. 2013. https://www.eff.org/deeplinks/2013/08/nsa-spying-three-pillars-government-trust-have-fallen

36 Timm, Trevor. "A Guide to the Deceptions, Misinformation, and Word Games Officials Use to Mislead the Public About NSA Surveillance." 14 Aug. 2013. https://www.eff.org/deeplinks/2013/08/guide-deceptions-word-games-obfuscations-officials-use-mislead-public-about-nsa

37 Electronic Frontier Foundation. "The Government's Word Games When Talking About NSA Domestic Spying." https://www.eff.org/nsa-spying/wordgames

Similarly, the Chief Judge of the FISC has confirmed that the court cannot conduct broad oversight of the NSA.[38]
Recently the government has allowed service providers to release very general information about requests for information by the NSA, but those are still grossly insufficient.

Integrity of Communications and Systems

The Necessary and Proportionate Principles state that, "States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes."

The extent to which the NSA, GCHQ, and others have done just that has been one of the most significant revelations this year. They have secretly undermined the global communications infrastructure and services, as specified in the MUSCULAR operation described above.[39] They have obtained private encryption keys for commercial services relied upon by individuals and have, in general, undermined international security standards. The assumption underlying such efforts—that no communication can be permitted to be truly secure—is inherently dangerous. It leaves people vulnerable on communication systems known to be under attack by criminals and state actors alike. Degrading or disabling the security of hundreds of millions of people—who rely on secure technologies for confidential communication and financial transactions—in order to enhance the surveillance capabilities of the intelligence community is extremely shortsighted and grossly inconsistent with the Principles.

Extraterritorial Application of Human Rights Law

The US contends that its human rights treaty obligations under the ICCPR do not apply to its actions abroad, a view that defeats the object and purpose of the treaty. The Human Rights Committee rejected the United States' position and reiterated that the United States has an extraterritorial duty to protect human rights—including the right to privacy—to its actions abroad regardless of the nationality or location of the individuals.[40] The United States asserts control over any data held by companies based in the United States regardless of where the data may be physically stored. Thus, the US controls data located outside the US, even as it argues that it is not responsible for any interference with privacy that results.[41]

38 Leonnig, Carol D. "Court: Ability to police U.S. spying program limited." 16 Aug. 2013. http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html

39 Auerbach, Dan and Kurt Opsahl. "Crucial Unanswered Questions about the NSA's BULLRUN Program." 9 September, 2013. https://www.eff.org/deeplinks/2013/09/crucial-unanswered-questions-about-nsa-bullrun-program

40 "Human Rights Committee considers report of the United States, 110th session." 14 March 2014. http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=14383&LangID=E

41 Human Rights Watch and Electronic Frontier Foundation—Joint Shadow Report to the Human Rights Committee. 14 Feb. 2013. https://www.eff.org/files/2014/03/12/hrweffsubmission_on_privacy_us_ccpr_final.pdf

Given the extraordinary capabilities and programs of the US to monitor global communications, it is essential that the protection of privacy applies extraterritorially to innocent persons whose communications the NSA scans or collects. Without such protections, the object and purpose of the United States' international human rights obligations—with regard to the right of privacy in borderless global communications—would be defeated.[42]

EFF and Human Rights Watch have urged the Human Rights Committee to—given the extraordinary capabilities and programs of the United States to monitor global communications—advise the United States that it must acknowledge its obligations, with respect to the right of privacy, apply extraterritorially to persons whose communications it scans or collects. To accept otherwise would defeat the object and purpose of the ICCPR with regard to the privacy of borderless, global digital communications. Although the precise scope of US surveillance programs is unknown, a steady stream of press revelations suggests that these programs may be sweeping in communications and personal data of potentially millions of people worldwide.

Facts: Three major shifts in technology have made it especially easy for the US to conduct broad, systematic surveillance of individuals outside its borders.[43]

Much of the world's digital communications flow through fiber optic cables inside the US, even when such communications do not involve a US-based Internet user. Through cooperative agreements, the US appears to have access to information gathered in bulk by foreign intelligence services, including GCHQ in the U.K.
Many of the world's most popular Internet companies (email providers, social media services, etc.) are US-based companies. These firms store and process global user data inside the US, making such data more readily available to the US government. The US also believes that it has jurisdiction over all of these companies' operations, wherever they occur, since they are incorporated in the US. This is true even when the user is not in the US and is not communicating with anyone in the US.
Global communications have increased and shifted a substantial degree to Internet-enabled services such as email, social media, voice services, and other online tools. Cross-border communication is now instant, commonplace, and cheap (compared to international phone calls). The Internet has also enabled users to exercise the right to freedom of expression and has provided access to knowledge and information on an unprecedented global scale. Storage and analysis of digital data across borders is also possible on an unprecedented scale, and at a relatively low cost, lowering barriers to present and future mass surveillance.

42 *Id.*

43 Electronic Frontier Foundation and Human Rights Watch, "Supplemental Submission to the Human Rights Committee During its Consideration of the Fourth Periodic Report of the United States." 14 Feb. 2014. https://www.eff.org/document/eff-and-human-rights-watch-joint-submission-human-rights-committee

Equal Privacy Protection For Everyone

US surveillance law violates the Principle of Illegitimacy because it involves unjustified discrimination against non-US persons—providing less favorable standards to them than its own citizens. Human rights law must protect "everyone," meaning all human beings. As the Universal Declaration of Human Rights has stated, ""All human beings are born free and equal in dignity and rights." Indeed, everyone must be entitled to equal protection under the law and the Constitution.

Conclusion

This document can provide only the broadest overview of how NSA surveillance programs fail to comport with their international human rights obligations, including the Necessary and Proportionate Principles. There is still more analysis to be done.

Nonetheless, we hope the Principles and this document will together serve as an initial overview for understanding how the US, and any other state operating mass surveillance programs on innocent citizens in secret, fail to meet current international human rights standards.

We hope that the Necessary and Proportionate Principles provide guidance to the States on how to implement their obligations to protect human rights in light of our new digital environment, and allow our communication networks to live up to the promise of a global interconnected infrastructure that protects, not undermines, our fundamental freedoms.