December 17, 2015

US Surveillance Law, Safe Harbor, and Reforms Since 2013

Peter Swire[1]

Executive Summary:

This White Paper is a submission to the Belgian Privacy Authority for its December 18, 2015 Forum on "The Consequences of the Judgment in the *Schrems* Case."[2] The Forum discusses the decision by the European Court of Justice in *Schrems v. Data Protection Commissioner*[3] that the EU/US Safe Harbor was unlawful under the EU Data Protection Directive, particularly due to concerns about US surveillance law.

For the Forum, I have been asked to comment on two issues:

1) Is US surveillance law fundamentally compatible with E.U. data protection law?
2) What actions and reforms has the US taken since the Snowden revelations began in June 2013?

The White Paper draws on my background as a scholar of both EU data protection law and US surveillance law. It addresses serious misunderstandings of US national security law, reflected in official statements made in the *Schrems* case and elsewhere. It has three chapters:

(1) *The fundamental equivalence of the United States and EU member States as constitutional democracies under the rule of law.* In the *Schrems* decision, the US was criticized for failing to ensure "a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order." This chapter critiques that finding, instead showing that the United States has strict rule of law, separation of powers, and judicial oversight of law enforcement and national security

[1] **Peter Swire** is the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business and a Senior Fellow of the Future of Privacy Forum. He is Senior Counsel with the law firm of Alston & Bird, LLP; nothing in this document should be attributed to any client of the firm. Further biographical information and acknowledgments are at the end of this White Paper.

[2] https://www.privacycommission.be/en/events/forum-consequences-judgment-schrems-case. The Belgian Privacy Commission is studying these issues for the broader group of European privacy regulators in the Article 29 Working Party. The level of EU skepticism of US surveillance law practices is reflected in the title of my panel: "Law in the EU and the US: impossible coexistence?"

[3] The ECJ opinion in *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14 (October 2015), available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=127557

surveillance, which together make the US legal order "essentially equivalent" to the EU legal order.

(2) *The Section 702 PRISM and Upstream programs are reasonable and lawful responses to changing technology.* The Advocate General's opinion in the *Schrems* case said that the PRISM program gave the NSA "unrestricted access to mass data" stored in the US, and that Section 702 enabled NSA access "in a generalised manner" for "all persons and all means of electronic communications." This chapter refutes those claims, which appear to be based in part on incorrect stories in the press. Instead, the Section 702 programs operate with judicial supervision and subject to numerous safeguards and limitations. They examine the communications only of targeted individuals, and only for listed foreign intelligence purposes. The total number of individuals targeted under Section 702 in 2013 was 92,707, a tiny fraction of Internet users in the EU or globally.

(3) *The US Congress and executive branch have instituted two dozen significant reforms to surveillance law and practice since 2013.* The *Schrems* decision said that US privacy protections must be evaluated in the "current factual and legal context," but did not address the numerous changes put in place since 2013. This chapter provides a readable explanation of each of these actions, which together constitute the biggest set of pro-privacy actions in US surveillance law since creation of the Foreign Intelligence Surveillance Act in 1978.

Chapter 1

The Fundamental Equivalence of the United States and EU Member States as Constitutional Democracies Under the Rule of Law

This chapter addresses the most basic requirement of the European Court of Justice (ECJ) in the *Schrems* decision, that the United States must ensure "a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order."[4] In the wake of the *Schrems* decision, there are now serious debates in the EU about whether any transfer of personal data to the US can be considered "adequate" under the requirements of the Data Protection Directive.[5] If the European legal regime makes a firm finding that the United States lacks the necessary legal order, then transfers of personal data may be essentially blocked, affecting large portions of trans-Atlantic commerce and communication.

This chapter seeks to explain the US system of law and surveillance to a European audience. The chapter stresses this point: *the fundamental equivalence of the United States and EU Member States as constitutional democracies under the rule of law.* The United States has its Constitution, continually in effect since 1790. The US has deeply established rule of law, separation of powers, and judicial oversight of both law enforcement and national security surveillance. For Europe to decide that the US "legal order" is unacceptable and deficient -- requiring blocking of most or all data transfers -- would be a consequential judgment, and one not supported by the facts. Among the many problems with such a decision, Europe would have to determine what other countries in the world have a constitutional law and practice that is the same as, or less protective than, the United States – such countries would logically also be ineligible to receive data transfers from the EU.

The discussion here of "fundamental equivalence" is different than a country-by-country comparison of the details of US surveillance law compared to the surveillance law of the 28 EU Member States. Others undoubtedly will present reports about whether the details of US law are "essentially equivalent" to the details of surveillance in the Member States. The discussion here of "fundamental equivalence" gives a deeper meaning to the ECJ's discussion of "essential

---

[4] Paragraph 96, 98, and 107 of the *Schrems* decision, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=127557.

[5] For instance, along with doubts about the validity of the Safe Harbor, German data protection authorities have questioned the legality of transfers of personal data to the US under model contracts or Binding Corporate Rules. The German DPA position paper is available, in German, at https://www.datenschutzzentrum.de/artikel/967-Positionspapier-des-ULD-zum-Safe-Harbor-Urteil-des-Gerichtshofs-der-Europaeischen-Union-vom-6.-Oktober-2015,-C-36214.html . A summary of the position paper is located at http://www.dataprivacymonitor.com/enforcement/german-data-protection-authorities-limit-use-of-alternative-data-transfer-mechanisms-in-light-of-safe-harbor-decision/

equivalence" – in its "essence" does the United States legal system provide protection for fundamental rights that is essentially equivalent to the Member States? At the basic, fundamental, and constitutive level, does the US legal system meet the minimum standard for protection of rights under the legal systems of any of the Member States?

As a law professor who has long studied both US and EU law,[6] my answer is a clear yes. To explain the fundamental equivalence of the US legal system, the chapter provides a brief introduction to the US as a constitutional democracy under the rule of law. It next explains the way that the Fourth Amendment to the US Constitution, governing searches and seizures, has been applied to wiretaps and changing technology over time in law enforcement cases. Then, the discussion turns to the related regime for foreign intelligence and national security wiretaps and surveillance. For both law enforcement and national security surveillance, independent judges with life tenure have thoroughly reviewed government surveillance programs, and have assured that legal protections are updated to match changing communications technology.

Some readers who are more familiar with the US legal system and its surveillance laws may decide to skip ahead to Chapter 2, concerning the Section 702 PRISM and Upstream programs, and Chapter 3, listing 25 US actions and legal changes in the surveillance sphere since the Snowden stories began in June 2013. This chapter provides some basic information on US constitutional and surveillance law, however, because the idea and the fact of fundamental equivalence has not been prominent to date in discussions related to the *Schrems* Safe Harbor decision.

A. The United States is a Constitutional Democracy Under the Rule of Law.

Readers of this White Paper will generally agree, I hope, that the United Sates is a constitutional democracy under the rule of law. The United States Constitution, which was ratified in 1790, creates three branches of government. The separation of the legislative, executive, and judicial branches matches the views of Montesquieu in his 1748 treatise on "The Spirit of the Laws" -- divided power among the three branches protects "liberty" and guards against "tyrannical" uses of power.[7] Under

[6] For instance, I was a student at L'Institut d'Études Européennes in Brussels in 1980-1981. I was the lead author of a book on EU data protection law in 1998. Peter Swire & Robert Litan, *None of Your Business: World Data Flows, E-Commerce, and the European Privacy Directive* (Brookings Institution, 1998). See also Peter Swire, "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet," 32 The International Lawyer 991 (1998) (analyzing choice of law issues under the EU Data Protection Directive), available at http://ssrn.com/abstract=121277; "Peter Hustinx and Three Clichés About E.U.-U.S. Data Privacy," in *Data Protection Anno 2014: How to Restore Trust?* (Hielke Hijmans & Herke Kranenborg ed.) (Intersentia 2014), available at http://ssrn.com/abstract=2404258.

[7] "When legislative power is united with executive power in a single person or in a single body of the magistracy, there is no liberty, because one can fear that the same monarch or senate that makes tyrannical laws will execute them tyrannically. Nor is there liberty if the power of judging is not separate from legislative power and from executive power. If it were joined to legislative power, the

the US Constitution, Congress is elected by the people; the President is elected to no more than two four-year terms; and federal judges are nominated by the executive, confirmed by the legislature, and appointed for life to ensure their independence.

The Bill of Rights to the United States Constitution specifically enumerates provisions to protect freedoms and privacy of individuals. Most important for surveillance issues, the Fourth Amendment limits the government's ability to conduct searches and seizures, and warrants can issue only with independent review by a judge. The Fourth Amendment governs more than simply a person's home or body; its protections apply specifically to communications, covering a person's "papers and effects."[8] Other fundamental rights and safeguards the Bill of Rights include: the First Amendment's protection of freedom of speech and freedom of association;[9] the Third Amendment's protection of the privacy of the home, by prohibiting the quartering of soldiers within a person's home;[10] and the Fifth Amendment's protection of the privacy of a person's thoughts, specifically by prohibiting the government from making persons testify about their own thoughts to incriminate themselves.[11]

B. Fundamental Protections Related to Law Enforcement Surveillance

To address changing technology, judges with life tenure have developed detailed case law concerning the Fourth Amendment, with somewhat different rules for law enforcement uses (crimes) and national security (foreign intelligence).

---

power over the life and liberty of the citizens would be arbitrary, for the judge would be the legislator. If it were joined to executive power, the judge could have the force of an oppressor. All would be lost if the same man or the same body of principal men, either of nobles, or of the people, exercised these three powers: that of making the laws, that of executing the laws, that of executing public resolutions, and that of judging the crimes or the disputes of individuals." Montesquieu, Book 11 Chapter 6 – On the Constitution of England. http://oll.libertyfund.org/titles/837

[8]The Fourth Amendment to the United States Constitution reads, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." https://www.law.cornell.edu/constitution/fourth_amendment (text); see http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 (explanation)

[9]The First Amendment to the United States Constitution reads, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." https://www.law.cornell.edu/constitution/first_amendment

[10]The Third Amendment to the United States Constitution reads, "No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law." https://www.law.cornell.edu/constitution/third_amendment (text)

[11]The Fifth Amendment to the United States Constitution reads, "No person . . . shall be compelled in any criminal case to be a witness against himself." https://www.law.cornell.edu/constitution/fifth_amendment (text)

As many have described, the Supreme Court has announced strict rules under the Fourth Amendment for wiretaps.[12] Initially, a closely divided Supreme Court in 1928 held that the Fourth Amendment did not apply, because the wiretap was done "in public" at the telephone poll.[13] Soon after, the Congress passed a law regulating wiretaps.[14] In the 1960's, the Supreme Court reversed that decision in the famous *Katz* and *Berger* cases, and set forth detailed requirements for law enforcement wiretaps.[15] Congress enacted those protections in 1968 in Title III of that year's crime bill, including strict minimization requirements and the requirement that wiretaps be used only when other investigative methods would not succeed.[16]

As an important part of the overall enforcement of the Fourth Amendment, the Supreme Court developed the "exclusionary rule," so evidence from an illegal search could not be used in court.[17] In addition, the Court barred evidence that was "the fruit of a poisonous tree" – additional evidence similarly could not be used in court if it was derived from an illegal search.[18]

In recent years, three Supreme Court cases illustrate the continuing judicial scrutiny of surveillance practices in light of changing technology:

1. *Riley v. California* (cell phones).[19] The longstanding rule has been that police can search a person "incident to arrest" – they can go through the person's pockets to spot possible weapons or evidence. The government took the position that this rule applied to cell phones. In 2014, the Supreme Court unanimously disagreed, holding that a judicial warrant was needed before police could search the contents of the cell phone. The Court said "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." In short, the Court updated fundamental rights protections to adapt to the changing technology of the cell phone.
2. *United States v. Jones* (search conducted in public).[20] The longstanding rule has been that police can "tail" a suspect in public – they can observe where a suspect goes. Police had also placed tracking devices on objects – the Supreme Court had previously ruled that the tracking device couldn't enter

[12] One discussion of the history of law enforcement and national security wiretaps is in Peter Swire, "The System of Foreign Intelligence Surveillance Law," 72 *Geo. Wash. L. Rev.* 1306 (2004), available at http://ssrn.com/abstract=586616.
[13] Olmstead v. United States, 277 U.S. 438 (1928). Justice Brandeis wrote a famous dissent, which was essentially adopted by the Supreme Court in the 1968 *Katz* case.
[14] Communications Act of 1934, Pub. L. No. 97-259 (codified at 47 U.S.C. § 307).
[15] *Katz v. United States*, 389 U.S. 347 (1967); *Berger v. New York*, 388 U.S. 41 (1967).
[16] Omnibus Crime Control and Safe Streets Act of 1969, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified at 18 U.S.C. § § 2510-2521.)
[17] Mapp v. Ohio, 367 U.S. 643 (1961).
[18] Wong Sun v. U.S., 371 U.S. 471 (1963).
[19] Riley v. California, (United States Supreme Court decision, June 2014) http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.
[20] United States v. Jones, 132 S. Ct. 945, 565 U.S. __ (2012).

the home without a warrant, but had never prohibited tracking a suspect in public. In 2012, the Court unanimously held that a warrant was required for a tracking device put on a suspect's car for 30 days. One problem was that the police were "trespassing" on the suspect's car when they attached a device. Justices wrote at length, however, about the constitutional protections that were needed to prevent long-term and widespread surveillance in public, in light of changing technology.

3. *Kyllo v. United States* (search of house conducted from the street).[21] Longstanding doctrine has permitted the police to gather evidence that is in "plain view." In this 2001 case, the police used a thermal imaging device to detect a high level of electricity usage in a house where marijuana was being grown. The Court stated: "Where, as here, the Government uses a device that is not in general use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." This holding constrained police surveillance even when the evidence was gathered from the street rather than entering the home.

In conclusion on the rules on law enforcement surveillance, the independent judiciary in the US has a long practice, as well as prominent recent examples, of constraining surveillance conducted by new technologies.

C. Fundamental Protections Related to National Security Surveillance

The US rules applying to national security surveillance are different in certain ways from the law enforcement rules, but multiple, significant constitutional and statutory protections apply even in the national security setting.

The Supreme Court's discussion of national security wiretaps notably began in the 1967 *Katz* case, where the Court announced Fourth Amendment requirements for law enforcement wiretaps. With regard to national security, the Court stated: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented in this case."

The Supreme Court addressed the lawfulness of national security wiretaps in 1972 in *United States v. United States District Court*, generally known as the "Keith" case after the name of the district court judge in the case. The defendant was charged with the dynamite bombing of an office of the Central Intelligence Agency. In what the New York Times referred to as a "stunning" victory for separation of powers, the Supreme Court concluded that "Fourth Amendment freedoms cannot be properly guaranteed if domestic security surveillance may be conducted solely

[21] Kyllo v. United States, 533 U.S. 27 (2001).

within the discretion of the Executive Branch."[22] The Court held that, for wiretaps or other electronic surveillance of domestic threats to national security, the government must first receive a judicial warrant. The Court expressly withheld judgment "on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country."[23]

The modern rules for national security surveillance were shaped by Watergate. The break-in to the office in the Watergate building was an example of a classic threat from unchecked executive power – an intrusion into the office of the opposing political party. Following the resignation of President Nixon in 1974, Congress passed the Privacy Act of 1974, creating new protection against misuse of personal information by federal agencies. In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA), a path-breaking legal structure to address the problem of secret surveillance in an open society.

I have previously written in detail about the numerous legal provisions in FISA.[24] A key point, for present purposes, is that the law created the Foreign Intelligence Surveillance Court (FISC), staffed by independent federal judges with lifetime tenure. Wiretaps and electronic surveillance for foreign intelligence purposes, conducted within the US, could only be done with approval by a FISC judge. Except for short-term emergency orders, the President, the Attorney General, and the FBI could no longer do national security wiretaps on their own – the judges served as a crucial check on the executive branch. Safeguards for FISA orders include:

- Requirement for high-level approval within the Department of Justice for any FISA order;
- Minimization procedures to reduce the effects on persons other than the targets of surveillance;
- Provision for electronic surveillance for a limited time, with the opportunity to extend the surveillance; and
- Requirement for details to the judge concerning the targets of the surveillance and the nature and location of the facilities placed under surveillance.

Congress created institutional checks on the issuance of the secret FISA wiretaps. For instance, Congress created the Senate and House Intelligence Committees, which receive classified briefings about intelligence surveillance. The

[22] Morrison, Trevor, "*The Story of the United States v. United States District Court (Keith*): The Surveillance Power," at 2 (Columbia Policy Law & Legal Theory Working Papers, 2008) , http://lsr.nellco.org/cgi/viewcontent.cgi?article=1047&context=columbia_pllt

[23] The Court specifically invited Congress to pass legislation creating a different standard for probable cause and designating a special court to hear the wiretap applications. Congress accepted this invitation in FISA.

[24] Peter Swire, "The System of Foreign Intelligence Surveillance Law," 72 *Geo. Wash. L. Rev.* 1306 (2004), available at http://ssrn.com/abstract=586616.

Attorney General must report to these committees every six months about FISA electronic surveillance, including a description of each criminal case in which FISA information has been used for law enforcement purposes. The Attorney General also must make an annual report to Congress and the public about the total number of applications made for orders and extensions of orders, as well as the total number that were granted, modified, or denied.

Chapter 2 of this White Paper discusses the judicial oversight and safeguards under the Section 702 PRISM and Upstream programs. Chapter 3 discusses numerous actions and reforms undertaken since 2013 to promote oversight, transparency, and democratic accountability for national security surveillance.

D. Conclusion

Under the Data Protection Directive, transfers of personal data can be made to third countries if there is "adequate" protection, which the ECJ has stated means "essentially equivalent" protection. One aspect of this essential equivalence determination for Safe Harbor 2.0 will concern specific provisions of law, such as data subject access rights or right to have investigation by an independent data protection authority in the data subject's country. I leave that sort of essential equivalence analysis to other authors.

The discussion here has instead focused on the *Schrems* discussion of essential equivalence to the protections guaranteed in the "EU legal order." That comparison requires understanding of the "US legal order." As discussed in this chapter, both the US and EU Member States are constitutional democracies under the rule of law. The US has a long tradition of, and recent examples of, independent judges updating fundamental rights protections to adapt to changing technology. The system for governing national security surveillance features the vital principles of oversight, transparency, and democratic accountability. The latter was illustrated in 2015 with passage of the USA Freedom Act limiting national security surveillance.

Fundamental rights advocates in the EU and the US often propose ways that particular rights can be better protected. There is no claim here that the legal order in either the EU or US protects human rights in the best possible way. The key point instead is that both legal orders are essentially equivalent in their method of democratic governance with constitutional protections. Dismissing the US legal order as fundamentally flawed would be contrary to the facts and would cause major disruptions to commerce and communications between allied nations.

Chapter 2

The Section 702 PRISM and Upstream Programs are Reasonable and Lawful Responses to Changing Technology.

This chapter explains and analyzes the PRISM and Upstream programs under Section 702. Although there are specific issues where I believe current law should be improved, Section 702 overall is a reasonable and lawful response to technological changes.

This chapter explains the legal structure of Section 702 before providing more detail about the PRISM and Upstream programs. Section 702 applies to collections that take place within the US, and only authorizes access to the communications of targeted individuals, for listed foreign intelligence purposes. The independent Privacy and Civil Liberties Oversight Board, after receiving classified briefings on Section 702, came to this conclusion as part of its 196 page report: "Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse."[25]

We now know, based on declassified documents, that the Foreign Intelligence Surveillance Court carefully reviews NSA's implementation of Section 702 and has required the government to modify aspects of its procedures to address compliance incidents that have been reported by the Government to the Court. In my view, these declassified opinions show the willingness and ability of independent judges to hold intelligence agencies accountable if they stray from the law.

The Section 702 programs have received stern criticism from European officials in the *Schrems* case. Notably, the Advocate General's Opinion included the following statements (with emphasis supplied): "According to the Snowden revelations, the NSA established a programme called 'PRISM' under which it obtained *unrestricted access to mass data* stored on servers in the United States owned or controlled by a range of companies active in the Internet and technology field, such as Facebook USA."[26] Later, the Opinion states as fact: ''Indeed, the access of the United States intelligence services to the data transferred covers, *in a comprehensive manner*, all persons using electronic communications services,

[25] PCLOB Report 702, at 2.
[26] http://www.scl.org/site.aspx?i=ne44089.

without any requirement that the persons concerned represent a threat to national security." The Opinion says the access covers "*in a generalised manner, all persons and all means of electronic communicatio*n and all the data transferred, including the content of the communications, without any differentiation, limitation or exception according to the objective of general interest pursued." It adds that, for information transferred by a company such as Facebook to the U.S., there is "*mass, indiscriminate surveillance*."

I quote the Advocate General's Opinion in detail because of the large gap between these statements and how Section 702 actually operates. One difficulty, described in detail here, is that the original Washington Post story about PRISM was inaccurate and subsequently corrected. Observers including the Fundamental Rights Agency of the European Union have now recognized the factual mistakes. Based on the corrected facts, the Fundamental Rights Agency[27] and the US Privacy and Civil Liberties Oversight Board have found that PRISM is not a bulk collection program, but instead is based on the use of targeted selectors such as emails.

The Upstream program similarly acquires only targeted communications. From a recently declassified opinion of the Foreign Intelligence Surveillance Court, we now know that the number of electronic communications acquired through Upstream in 2011 was only about 10 percent of the number acquired by PRISM. We also know, based on the same opinion, that the FISC has carefully reviewed NSA's implementation of Section 702 and has required the government to modify aspects of its procedures to address compliance incidents reported by the Government to the Court. In my view, this and other declassified opinions show the willingness and ability of independent judges to hold US intelligence agencies accountable if they stray from the law.

People of good will and intelligence can disagree on what constitutes a reasonable approach to changing technology. Chapter 3 discusses Section 702 reforms that have been put in place since 2013. President Obama's Review Group on Intelligence and Communications Technology, on which I served, made recommendations about Section 702 that have not been made to date, some of which can only be made by Congress, which will review the law when it sunsets in 2017.[28] I am not saying Section 702 is perfect, but it is perfectly clear that the rule of law applies under statutory, executive, and judicial oversight, and Section 702 is not "unrestrained."

[27] European Union Agency for Fundamental Rights, "Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU" (2015), at 17, available at http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

[28] Review Group Report, Recommendation 12, at 145-150.

A. The Legal Structure of Section 702.

The rationale for what is commonly referred to as Section 702 of FISA[29] evolved from the changing nature of international communications. Prior to the Internet, surveillance of communications between two people outside of the US took place outside of the US. For instance, a phone call between someone in France and someone in Pakistan could be collected either in France or Pakistan (or perhaps somewhere in between). Under US law, the Fourth Amendment of the US Constitution clearly applies to wiretaps that are made within the US. By contrast, these constitutional protections do not apply to communications between a French person in France and a Pakistani in Pakistan – they are not part of the community that has agreed to live under the governance of the US Constitution. Accordingly, collection of this type of information historically was outside of FISA's jurisdiction. As discussed further in Chapter 3, EU and other democracies have similarly given themselves greater freedom to do surveillance outside of their borders than within.

With the rise of the Internet, the facts changed. Now, the same communication between France and Pakistan quite possibly did pass through the United States -- much of the Internet backbone has been built in the US, and many communications thus route through the US. One legal question answered by Section 702 was how to govern foreign-foreign communications[30] when the intercept occurred within the US.[31] A related factual change concerned the growing use of US-based providers for webmail, social networks, and other services. This change meant that communications between two non-US persons more often would be stored within the US. In light of these factual changes, as well as technological issues affecting the previous statutory text,[32] Congress passed Section 702 of FISA in 2008.

The basic structure of Section 702 is that the Foreign Intelligence Surveillance Court must annually approve certifications by the Director of National Intelligence and the Attorney General setting the terms for Section 702 surveillance.[33] To target the communications of any person, the government must have a foreign intelligence purpose to conduct the collection and a reasonable belief

[29] "Section 702" refers to a provision in the Foreign Intelligence Surveillance Act Amendments Act of 2008, which revised the Foreign Intelligence Surveillance Act of 1978, available at https://www.govtrack.us/congress/bills/110/hr6304/text.

[30] This type of communication was historically handled under E.O. 12,333, available at http://www.archives.gov/federal-register/codification/executive-order/12333.html.

[31] This type of communication was historically governed by the stricter standards of FISA, available at https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286.

[32] Laura K. Donohue, "Section 702 and the Collection of International Telephone and Internet Content," 38 Harv. J. L. & Pub. Policy 117, 142 (2015) (discussing technical issues with FISA's definition of "electronic surveillance").

[33] For discussion of the numerous specific requirements in Section 702, see Laura K. Donohue, "Section 702 and the Collection of International Telephone and Internet Content", available at http://scholarship.law.georgetown.edu/facpub/1355/; see also NSA Director of Civil Liberties and Privacy Office Report, "NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" (April 2014), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf.

that the person is a non-US citizen located outside of the US.[34] Section 702 can provide access to the full contents of communications, and not just to/from information. The court annually reviews and must approve targeting criteria, documenting how targeting of a particular person will lead to the acquisition of foreign intelligence information. As discussed in Chapter 3, the administration has agreed to strengthen the targeting rules.[35] The court annually also approves minimization procedures, to cover the acquisition, retention, use, and dissemination of non-publicly available information about US persons.[36]

The Review Group discussed the following set of safeguards that accompany NSA access to information under Section 702. These safeguards show the enormous difference between "unrestricted access to mass data" and actual US law and practice:

1) Targeting must be for a valid foreign intelligence purpose in response to National Intelligence Priorities;
2) Targeting must be under a Foreign Intelligence Surveillance Court (FISC) approved Section 702 Certification and targeted at a person overseas;
3) All targeting is governed by FISC-approved targeting procedures;
4) Specific communications identifiers (such as a phone number or email address) are used to limit collections only to communications to, from, or about a valid foreign intelligence target;
5) Queries into collected data must be designed to return valid foreign intelligence (or, in the case of the FBI, foreign intelligence information or evidence of a crime) and overly broad queries are prohibited and supervised by the FISC;
6) Disseminations to external entities, included select foreign partners (such as E.U. member states) are made for valid foreign intelligence purposes; and
7) Raw data is destroyed after two years or five years, depending on the collection source.[37]

The PCLOB's report on Section 702 provides step-by-step examples about how these safeguards apply in practice.[38]

[34] Review Group Report, Appendix A.
[35] The changes include: (1) Revision of the NSA's targeting procedures to specify criteria for determining the expected foreign intelligence value of a particular target; (2) Further revision to require a detailed written explanation of the basis for the determination; (3) FISC review of the revised targeting procedures and requirements of documentation of the foreign intelligence finding; (4) Other measures to ensure that the "foreign intelligence purpose" requirement in Section 702 is carefully met; (5) Submission of the draft targeting procedures for review by the PCLOB (an independent agency with privacy responsibilities); and (6) Compliance, training, and audit.
[36] https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf
[37] RG Report, at Appendix B.
[38] PCLOB 702 Report, at 46.

To give perspective on Section 702, it provides more detailed legal restrictions than applied previously to foreign-foreign communications. Previously, if the US conducted surveillance overseas, to target foreign communications, the US Constitution and other laws did not limit US government activities.[39] Now, when the same two non-US persons communicate, and the communication is accessed within the US, any access to the contents must be done under a federal court order and the multiple safeguards of the Section 702 regime.

B. The PRISM program is not a bulk collection program.

The PRISM program became famous when it was publicly named in one of the first stories based on the Snowden documents. The initial story was incorrect in important respects, but those inaccuracies have been widely repeated. As found by independent European and US reviews, the actual PRISM program is not even a bulk collection program, much less the basis for "mass and indiscriminate surveillance" when data is transferred from the EU to the US.

The actual operation of PRISM is similar to data requests made in other settings to service providers. In PRISM collection, acting under a Section 702 court order, the government sends a directive requiring collection of certain "selectors," such as an email address. The directive goes to a United States-based service provider. The company lawyers have the opportunity to challenge the government request. If there is no appeal to the court, the provider is compelled to give the communications sent to or from that selector to the government.[40]

Widespread misunderstanding of PRISM traces to a Washington Post story that led with this statement: "The National Security Agency and the FBI are tapping *directly* into the *central* servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents, and connection logs that enable analysts to track a person's movements and contacts over time."[41] We now know

[39] Access to those communications, acquired overseas, would typically be governed by Executive Order 12,333, which is less strict than Section 702.

[40] PCLOB 702 Report, at 7.

[41] Barton Gellman, "U.S. intelligence mining data from nine U.S. Internet companies in broad secret program" *Washington Post*, June 6, 2013. (emphasis added), available at https://fg3qua.dm2302.livefilestore.com/y3mKC7oGF-GpV3F7dq9wjirtfXMk8TIfCYCDL59yJI0k24j_SqPf2jTlZTcEq1ZtVFSOaCKrPOuYarNeNJ3Ykt_NSBD_ut-_9oMMOXLdcMb6Np6Bx78sjfzftnHDswYoKzQUeeC81zjcldDgZSy3rCY7g/WaPo%20NSA%20report%20-%20heavy%20editing.pdf?psid=1. When the original version of the article was withdrawn from the *Washington Post*'s website on June 7, 2013 and replaced with a revised version, the headline of the article was also changed, explanation at https://pjmedia.com/blog/wapo-quietly-changes-key-details-in-nsa-story. The new headline read, "U.S, *British* intelligence mining data from nine U.S. Internet companies in broad secret program." (emphasis added), at https://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.
Gellman further asserted that, "[f]rom inside a company's data stream the NSA is capable of pulling out anything it likes."

that the government does not have direct access under the PRISM program, but instead serves legal process on the providers similar to other stored records requests.

The inaccuracies in the news story led to immediate responses. Technology companies named in the article[42] issued statements denying that the government had direct access to their servers to collect user data.[43] Within 24 hours, the *Washington Post* itself heavily edited the original story, but left the lead sentence intact.[44] In reviewing the events, prominent media sources soon reported the *Washington Post* account was inaccurate because each company had only responded to government requests for information after receiving a directive requiring them to do so.[45]

As can easily happen with press stories, the corrections never caught up with the original mistake. The mistake about direct access to servers was quoted in the High Court of Ireland's decision in *Schrems v. Data Protection Commissioner:*[46]

> "According to a report in *The Washington Post* published on 6th June 2013, the NSA and the Federal Bureau of Investigation ("FBI"): 'are tapping directly into the central servers of nine leading US internet companies, extracting audio and video chats, photographs, e-mails, documents and connection logs that enable analysts to track foreign targets….' According to the *Washington Post* the programme is code-named PRISM and it apparently enables the NSA to collect personal data such as emails, photographs and videos from major internet providers such Microsoft, Google and Facebook."[47]

The Advocate General to the European Court of Justice did not directly cite the *Washington Post* story, but relied on the mistaken view of the facts in saying: "According to those revelations, the NSA established a programme called 'PRISM' under which it obtained *unrestricted access to mass data* stored on servers in the United States owned or controlled by a range of companies active in the Internet and technology field, such as Facebook USA."[48] The opinion added that, for information

---

[42] The nine companies named were AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype, Yahoo, and YouTube.

[43] [Cite]

[44] [Cite]

[45] See http://www.engadget.com/2013/06/06/washington-post-nsa-fbi-tapping-directly-into-servers-of-9-lea/; http://www.cnet.com/news/no-evidence-of-nsas-direct-access-to-tech-companies/; http://www.businessinsider.com/washington-post-updates-spying-story-2013-6

[46] *Schrems v. Data Protection Commissioner*, 2014 IEHC 310, available at http://fra.europa.eu/en/caselaw-reference/ireland-high-court-ireland-2014-iehc-310

[47] *Schrems v. Data Protection Commissioner*, 2014 IEHC 310, available at http://fra.europa.eu/en/caselaw-reference/ireland-high-court-ireland-2014-iehc-310

[48] Paragraph 26 of the Advocate General's opinion in *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14 (September 2015), (emphasis added), available at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=168421

transferred by a company such as Facebook to the US, there is "mass, indiscriminate surveillance."[49]

These sensational but incorrect factual assertions are a close fit with the crucial statement by the European Court of Justice that the United States lacks "a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order."[50]

The correction has already been understood by leading European and US institutions. The European Union Agency for Fundamental Rights recently released a major report about surveillance by intelligence services, at the request of the European Parliament.[51] This report recognized the corrected view of PRISM. It cites an article by M. Cayford and others that stated: "The interpretation by *The Washington Post* and *The Guardian*[52] was that this meant these companies were collaborating with the NSA to give it a direct connection to their servers, to 'unilaterally seize' all manner of communications from them. This proved, however, to be incorrect."[53] The Agency for Fundamental Rights report agreed with the Cayford article statement that PRISM is "'a targeted technology used to access court ordered foreign internet accounts," and not mass surveillance.[54] The US Privacy and Civil Liberties Oversight Board, an independent agency that received classified information about the PRISM program, similarly concluded: "the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead the program consists entirely of targeting specific [non-U.S.] persons about whom an individualized determination has been made."[55]

---

[49] Id. at Paragraph 200.

[50] Paragraph 96 of the ECJ opinion in *Schrems*

[51] http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

[52] The Guardian article revealing the PRISM program also reported that this program gave the NSA direct access to the servers of major internet providers such as Google, Apple, Skye, and Yahoo. The slide speaks of PRISM "collection directly from the servers" of nine US internet service providers. The article is entitled, "NSA Prism program taps in to user data of Apple, Google, and others," available at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[53] M. Cayford, et al., "All Swept Up: An Initial Classification of NSA Surveillance Technology," at 645-46, available at http://www.crcnetbase.com/doi/abs/10.1201/b17399-9. The European Union Agency for Fundamental Rights report reviewed the PRISM program in light of the Cayford article, which found that "[t]he 'direct access' described … is access to a particular foreign account through a court order for that particular account, not a wholesale sucking up of all the information on the company's users." European Union Agency for Fundamental Rights , "Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU" (2015), at 17, available at http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

[54] European Union Agency for Fundamental Rights, "Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU" (2015), at 17, available at http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

[55] Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2014) at 111, available at https://www.pclob.gov/library/702-Report.pdf

The public also now has access to official statistics about the number of individuals targeted under Section 702. The US intelligence community now releases an annual Statistical Transparency Report,[56] with the statistics subject to oversight from Congress, Inspector Generals, the FISC, the PCLOB, and others.[57] For 2014, there were 92,707 "targets" under the Section 702 programs, many of whom are targeted due to evidence linking them to terrorism.[58] That is a tiny fraction of US, European, or global Internet users. It demonstrates the low likelihood of the communications being acquired for ordinary citizens.[59]

C. The Upstream program accesses fewer electronic communications than PRISM

The Upstream program gains emails and other electronic communications from the Internet backbone, and thus the European Union Agency for Fundamental Rights noted that the same Cayford article that found PRISM not to be "mass surveillance" has called the Upstream program "mass surveillance."[60] Upon examination, I believe a better view is that the legal rules that authorize Upstream mean that it is a targeted program as well. Indeed, the targeting and minimization procedures for Upstream collection are the same as or stronger than those that are applied to PRISM collection. A declassified FISC opinion found that over 90% of the Internet communications obtained by the NSA in 2011 under Section 702 actually resulted from PRISM, with less than 10% coming from Upstream.[61] Upstream collection takes place with the same targeted selector process that is used for PRISM. In short, given the positive findings from European experts about the PRISM program, there is a strong basis for rejecting the conclusion that Upstream is "mass surveillance," given its much smaller scale.

---

[56] The first two have been released: Calendar Year 2014 Transparency Report; Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2014 - April 22, 2015, at http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014; 2013 Transparency Report; Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2013 - June 26, 2014, at http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.

[57] For a listing of the multiple oversight entities, see Review Group Report, Appendix C.

[58] The statistical reports define "target" in detail, and the number of individuals targeted is lower than the reported number, to avoid any possible understatement of the number of targets.

[59] The 2014 Statistical Transparency Report reiterates the targeted nature of the surveillance: "Given the restrictions of Section 702, only selectors used by non-U.S. persons reasonably believed to be located outside the United States and who possess, or who are likely to communicate or receive, foreign intelligence information that is covered by an approved certification may be tasked."

[60] European Union Agency for Fundamental Rights, "Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU" (2015), at 17, available at http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf

[61] The analysis of Judge Bates' opinion is in the PCLOB Section 702 report, at 33-34. I am not aware of a similar quantitative comparison of PRISM and the Upstream program for telephone communications, but the discussion here of filtering and acquisition of targeted communications applies in the same way to both telephone and electronic communications.

1. How the Upstream Technology Works

The Upstream program is clearly explained in the PCLOB's report on Section 702.[62] The NSA may target non-US persons by tasking specific selectors, such as email addresses or telephone numbers, and may not use key words or the names of targeted individuals.[63]

As discussed at the start of this Chapter, the Upstream program is a response to changing technology. As the Internet developed, a large portion of the Internet backbone passed through the United States, meaning that many foreign-foreign communications could be accessed by surveillance done inside the US. Previously, foreign-foreign communications would have been accessed outside of the US, where the US Constitution and various laws are less strict than for access inside the US. The Upstream program, like the PRISM program, was authorized by the FISC under Section 702 as a way to apply the statute's safeguards to communications accessed in the US.

The PCLOB report explained the key role of a filter under Section 702, including for the Upstream program: "To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector."[64] Under Section 702, the filter selects only the communications that match the approved selectors, such as emails. Those emails make it through the filters, and are stored for access by the NSA. The information that doesn't make it through the filters is never accessed by the NSA or anyone else.[65]

Diagram 2-2 is taken from a US National Research Council report on "Bulk Signals Analysis: Technical Options." The diagram can be used to illustrate the role of the filter in the Upstream program. At the left side of the diagram, signals go through the Internet backbone. The signal is split ("extract") and then goes through the filter. The filter only allows authorized messages to pass through, based on "discriminants" or "selectors" such as email address. Authorized messages go into storage. At this point, for the first time, the messages can be queried. That is, under

[62] PCLOB Report on 702, at 36-39.

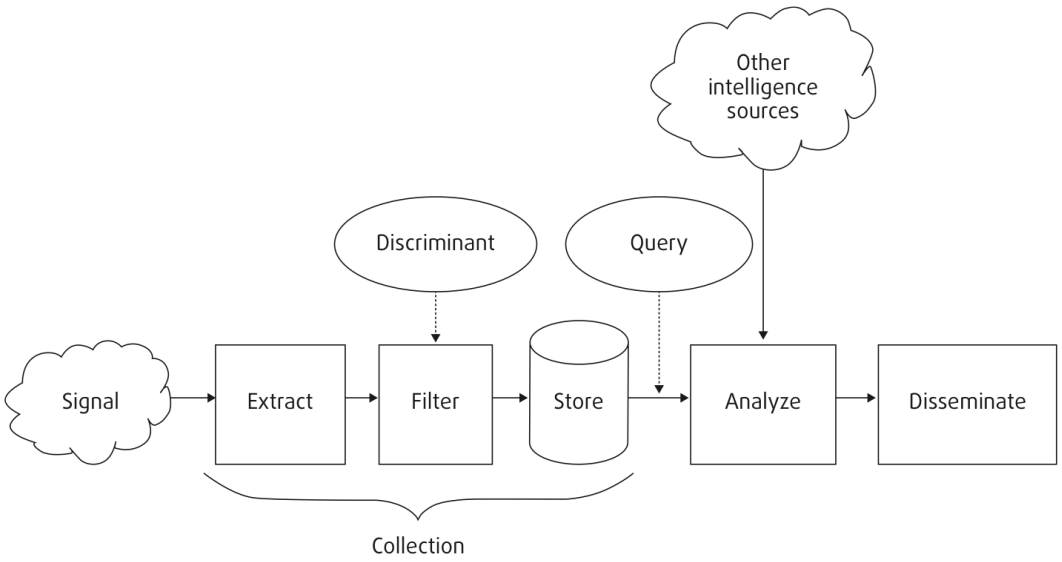
[63] The PCLOB writes: "The NSA may only target non-U.S. persons by tasking specific selectors to upstream Internet transaction collection. And, like other forms of Section 702 collection, selectors tasked for upstream Internet transaction collection must be specific selectors (such as an email address), and may not be key words or the names of targeted individuals." PCLOB Report at [cite]

[64] PCLOB report on 702, at 37.

[65] Some readers may not believe the NSA follows the rules and gains access only to approved communications that have made it through the filters. My own view is that the NSA has built a large and generally effective compliance program in recent years. As documented by the Review Group, multiple layers of oversight exist over these NSA actions, including oversight by judges, Congress, and the NSA Inspector General. Review Group Report, Appendices B and C. Systematic violation of the Section 702 rules would thus be highly risky for the NSA to undertake.

Upstream, only NSA employees can make queries, and they only have the ability to make queries on messages that have reached storage after filtering. Put another way, the NSA accesses only targeted communications, based on approved selectors.

Figure: Conceptual model of signals intelligence



Source: United States, National Research Council (2015), p. 28

Based on these technological realities, the National Research Council report noted that there are two differing conceptions of privacy for when data is acquired. One view (taken for instance by Cayford[66]) posits that violation of privacy occurs when the electronic signal is first captured, regardless of what happens to the signal after that point. The second view, which I share, is that processing the signal only for filtering purposes does not constitute mass surveillance. Access only to the filtered results, under rules such as those in Section 702, means that the communications of an individual are only retained if there is a match with a selector such as an email address.

The ultimate question is whether this sort of filtering, under law, should be permitted as a way to access communications flowing through the Internet. If the US (or an ally) has the technical ability to perform the filtering, and find high-value intelligence communications, society must decide whether to do so. Changing technology means that potentially vital national security information may be available, under a court order, as data flows through the system.

The PCLOB has written lengthy reports, based on classified information, on Section 215 telephone meta-data and on the Section 702 program, including

[66] M. Cayford, et al., "All Swept Up: An Initial Classification of NSA Surveillance Technology," at 644-45.

Upstream. The PCLOB found the former to be unlawful, bad policy, and not vital for national security. By contrast, the PCLOB unanimously came to a different verdict on the 702 program: (1) Section 702 "is not based on the indiscriminate collection of information in bulk";[67] (2) Section 702 meets the standard for reasonableness under the Fourth Amendment to the US Constitution;[68]; and (3) Section 702 has been effective at addressing international terrorism.[69]

2. Judge Bates' Declassified Opinion about Section 702 Illustrates Judicial Oversight of NSA Surveillance

One persistent question about US surveillance law has been whether there is independent judicial oversight of NSA practices. Based on recently-declassified opinions of the Foreign Intelligence Surveillance Court, the general public can now see the FISC holding NSA practices unlawful, and refusing to continue a surveillance program without modifications. As someone who has studied FISA for more than a decade, the declassified opinions match my prior view, that the FISC has often provided stricter oversight of surveillance practices than most on the outside have realized.[70] It is always been clear that judges on the FISC were independent in the sense that they have life tenure and cannot be removed from office except for good cause. Instead of the "indiscriminate surveillance" alleged by the Advocate General in *Schrems*, the declassified opinions show the FISC to be independent in the broader sense of applying judicial oversight to practices the judges find unlawful.

---

[67] The PCLOB found: "Unlike the telephone records program conducted by the NSA under Section 215 of the USA PATRIOT Act, the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized determination has been made. Once the government concludes that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information — and that this person uses a particular communications "selector," such as an email address or telephone number — the government acquires only those communications involving that particular selector." PCLOB Section 702 report at 111.

[68] The PCLOB "concludes that the core of the Section 702 program – acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules and multiple layers of oversight – fits within the "totality of the circumstances" standard for reasonableness under the Fourth Amendment, as that standard has been defined by the courts to date." PCLOB Section 702 report at 9.

[69] "Presently, over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. Monitoring terrorist networks under Section 702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics. In addition, the program has led the government to identify previously unknown individuals who are involved in international terrorism, and it has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries." PCLOB Section 702 report at 10.

[70] As with any court, reasonable people can differ on particular cases. I am critical of some of the declassified opinions, especially those upholding the lawfulness of the telephone meta-data program under Section 215.

A 2011 opinion by Judge Bates of the FISC found that NSA's minimization procedures were not adequate to deal with one portion of Upstream collection, and therefore required that those procedures be amended before he would authorize continuation of the program.[71] The controversy concerned NSA access to certain kinds of emails.[72] Judge Bates found that the Upstream program at that time did not satisfy the requirements of either FISA or the Fourth Amendment. He therefore refused to approve NSA's continuing acquisition of this category of emails.[73] Thereafter, the government substantially revised its procedures for handling the emails, and in November 2011 Judge Bates approved the future acquisition of those emails subject to the new minimization standards.[74] In addition, NSA took the additional step of deleting all previously acquired upstream communications.[75]

In my view, this and other declassified FISC decisions show vigorous and critical scrutiny by independent judges of the details of NSA surveillance.

D. Conclusion

The legal structure and implementation of PRISM and Upstream under Section 702 have been far more targeted and subject to oversight than the initial press reports claimed. With declassification of court orders, as well as documents such as the PCLOB report on Section 702, the general public and experts in Europe and the United States have a far stronger factual basis than prior to 2013 to debate what reforms may be appropriate when the law sunsets in 2017.

A key point of this chapter is that NSA acquisition of people's emails and other communications under Section 702 is not "pervasive" as has often been claimed. The Fundamental Rights Agency of the European Union has agreed with the PCLOB and others that the PRISM program is targeted rather than bulk collection. We know from declassified FISC documents that Upstream acquired less than 10 percent as many electronic communications in 2011 as PRISM, and so it is not pervasively acquiring electronic communications. Taken together, the total number of individuals targeted under Section 702 in 2013 was 92,707, a tiny fraction of total EU or global Internet users.

---

[71] *In re DNI/AG 702(g)*, Docket Number 702(i)-11-01 (FISC November 30, 2011) (Redacted version), available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf

[72] The problem arose where multiple emails were included in threads. For these "multi-communications transactions," the minimization procedures were not being applied in the way the Judge believed were necessary. Essentially, the Judge found that information was visible in the string of emails included within one email, in ways contrary to the minimization requirements.

[73] The court's opinion is discussed in detail in the Review Group's report, at 142.

[74] Report and Recommendation of the President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," at 142, available at https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[75] Report and Recommendation of the President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," at 142, available at https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Chapter 3

The US Has Taken Multiple and Significant Actions to Reform Surveillance Laws and Programs Since 2013

Since the Snowden disclosures in 2013, the US has undertaken at least two dozen significant actions to reform surveillance laws and programs. To explain these changes, this Chapter covers approximately 20 pages, a sign of the many (and detailed) reforms that have been put in place. The actions are:

A. Independent reviews of surveillance activities

1) Review Group on Intelligence and Communications Technology;
2) Privacy and Civil Liberties Oversight Board;

B. Legislative actions

3) Increased funding for the PCLOB;
4) Greater judicial role in Section 215 orders;
5) Prohibition on bulk collection under Section 215 and other laws;
6) Addressing the problem of secret law – declassification of FISC decisions, orders, and opinions;
7) Appointment of experts to brief the FISC on privacy and civil liberties;
8) Transparency reports by companies subject to court orders;
9) Transparency reports by the US Government;
10) Imminent passage of the Judicial Redress Act;

C. Executive branch actions

11) New surveillance principle to protect privacy rights outside of the US;
12) Protection of civil liberties in addition to privacy;
13) Safeguards for the personal information of all individuals, regardless of nationality;
14) Retention and dissemination limits for non-US persons similar to US persons;
15) Limits on bulk collection of signals intelligence;
16) Limits on surveillance to gain trade secrets for commercial advantage;
17) New White House oversight of sensitive intelligence collections, including of foreign leaders;
18) New White House process to help fix software flaws rather than use them for surveillance;
19) Greater transparency by the executive branch about surveillance activities;
20) Creation of the first NSA Civil Liberties and Privacy Office;
21) Multiple changes under Section 215;

22) Stricter documentation of the foreign intelligence basis for targeting under Section 702;
23) Other changes under Section 702; and
24) Reduced secrecy about National Security Letters.

These reforms exemplify the democratic response of the U.S. government to concerns raised surveillance and show a legal system responding to changes in technology.

A. Independent Reviews of Surveillance Activities

Issue: It is difficult to get informed and independent counsel about how to reform intelligence agencies. Many agency actions and programs are necessarily kept classified, to avoid revealing sources and methods for achieving their missions. To create one source of independent review, Congress established the Senate and House Intelligence Committees in the 1970's, in the wake of Watergate. Within the executive branch,[76] the most expert individuals generally have worked within the agencies that are being reviewed. That experience provides the expertise, but can also establish loyalties that are not easily set aside for purposes of critique and review.

Action: Beginning soon after June 2013, President Obama worked with two independent review efforts, staffed by knowledgeable people and able to get briefings at the TS/SCI level (Top Secret/Sensitive Compartmented Information), the highest level of security clearance. Reports have since been published, with detailed recommendations, from both the Review Group on Intelligence and Communications Technology ("Review Group") and the Privacy and Civil Liberties Oversight Board ("PCLOB").

(1) **Review Group on Intelligence and Communications Technology**

The Review Group was announced in August 2013, published its final report in December, and met with the President to receive its mission and discuss its recommendations.[77] The five members have diverse expertise: (1) Richard Clarke,

[76] Both houses of the US Congress, the Senate and the House of Representatives, have intelligence oversight committees. The mandate of these committees is to make continuing studies of the intelligence activities and to provide legislative oversight over the intelligence activities of the U.S. to assure that these activities are in conformity with the U.S. Constitution and laws. Members of these committees have access to classified intelligence assessments, access to intelligence sources and methods, programs, and budgets. For details on the U.S. Senate Select Committee on Intelligence, see http://www.intelligence.senate.gov/about. Information on U.S. House of Representatives Permanent Select Committee on Intelligence can be found at: http://intelligence.house.gov/.

[77] "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technology.," available at https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

former counter-terrorism and cybersecurity senior advisor to both President Clinton and George W. Bush; (2) Michael Morrell, former Deputy Director of the CIA, with thirty years of experience in the Intelligence Community; (3) Geoffrey Stone, eminent legal scholar on constitutional issues in time of crisis; (4) Cass Sunstein, the most-cited American legal scholar, and former Director of the Office of Information and Regulatory Affairs in the Office of Management and Budget; and (5) myself, with experience in areas including cybersecurity, foreign intelligence law, and privacy.

The Review Group's report was over 300 pages, made 46 recommendations, and has been reprinted as a book by the Princeton University Press. When President Obama made his major speech on surveillance reform in January 2014, the Review Group was told that 70 percent of its recommendations were being adopted in letter or spirit, and others have been adopted since. The Review Group's report received widespread attention in the press, especially this finding: "Our review suggests that the information contributed to terrorist investigations by the use of Section 215 telephony metadata was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional Section 215 orders."

(2) Privacy and Civil Liberties Oversight Board

By coincidence, the chair of the Privacy and Civil Liberties Oversight Board (PCLOB) started work the week the first Snowden story broke.[78] The PCLOB is the sort of independent oversight agency that has often been stressed by European data protection experts, with the same independent structure as the Federal Trade Commission. There are five members, no more than three from any political party, who serve a term of years. Members of the PCLOB and their staff receive TS/SCI security clearances and investigate and report on the counterterrorism activities of the US intelligence community.[79]

The PCLOB has distinguished members with relevant expertise: (1) David Medine, the Chair, was a senior FTC privacy official who helped negotiated the Safe Harbor; (2) Rachel Brand has been the Assistant Attorney General for Legal Policy, serving as chief policy advisor to the US Attorney General; (3) Beth Collins has also served as Assistant General for Legal Policy at the US Department of Justice; (4) Jim Dempsey is a leading surveillance expert in US civil society, working for many years at the Center for Democracy and Technology; and (5) Patricia Wald was a

---

The Review Group's task from the President was to find an approach "that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure." Id. The Report has been republished by the Princeton University Press, http://press.princeton.edu/titles/10296.html.

[78] I have sympathy for David Medine, the Chair, for trying to get his office furniture in place at the same time that the biggest intelligence story in decades hit the headlines.

[79] https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1283

judge on the Court of Appeals for the D.C. Circuit for twenty years, and has also served as a Judge on the International Criminal Tribunal for the former Yugoslavia.

Since 2013, the PCLOB has released detailed reports on the Section 215[80] and Section 702[81] surveillance programs, making numerous recommendations. Its central recommendations on the Section 215 telephone meta-data program were enacted in the USA Freedom Act, discussed below. Overall, PCLOB made 22 recommendations in its Sections 215 and 702 reports and virtually all have been accepted and either implemented or are in the process of being implemented.

In summary on the Review Group and the PCLOB, the overall reforms of the US intelligence system since Snowden have been informed by detailed reports, based on top-secret briefings. These reports have been written by independent groups who presented them to the President.

B. Legislative Actions

(3) Increased funding for the PCLOB.

Issue: At the time of the Snowden revelations, the PCLOB was a new agency whose Chair had just been sworn into office. The annual budget was too low to hire much staff.

Action: In 2014, Congress increased the PCLOB funding substantially, to $7.5 million and in 2015 to $10 million, bringing total staff to 32 plus five Board members.[82] This funding increase enables the PCLOB, going forward, to hire enough staff to continue to carry out its mandates and write detailed reports about intelligence community activities.

(4) Greater judicial role in Section 215 orders.

Issue: Under the Section 215 statute, as enacted in 2001, Foreign Intelligence Surveillance Court judges issued a general order to authorize the bulk collection of telephone meta-data. The decision to look at the information, however, was made by NSA employees, subject to oversight by the Department of Justice, based on a standard of "reasonable, articulable suspicion" that a telephone number was associated with terrorism.

Action: President Obama announced in 2014 that judicial approval would also be required for an NSA employee to look at the information. This approach was codified in the USA Act, passed in 2015, which also prohibited the bulk collection of

[80] https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf
[81] https://www.pclob.gov/library/702-Report.pdf
[82] The statistics are based on an interview with the PCLOB.

telephone metadata and required the queries to be submitted with court approval to the providers.[83]

As a separate amendment, the statute also required that judges will review the minimization procedures under Section 215 orders, to ensure that information, once accessed, is minimized to exclude records that are not foreign intelligence information, which previously were approved only by the Attorney General.[84]

(5) **Prohibition on bulk collection under Section 215 and other laws.**

Issue: Congress reacted, in the USA Freedom Act, to its concern that there could be bulk collection under a number of foreign intelligence authorities.

Action: The law prohibited bulk collection under three distinct authorities: (1) Section 215, for collection of "tangible things" (including phone records);[85] (2) FISA pen register and trap and trace authorities (to/from information about communications);[86] and (3) National Security Letters (phone, financial, and credit history records).[87] The law went beyond Section 215 orders to prevent the agencies from using alternative statutory authorities for bulk collection. These clear statements in law from the Congress plainly state the limits on appropriate use of Section 215 and other authorities.[88]

(6) **Addressing the problem of secret law – declassification of FISC decisions, orders, and opinions.**

Issue: A long-standing problem in the foreign intelligence area is how to avoid the development of secret law. Secret law is contrary to the basic theory of democracy, that citizens should govern themselves, and thus should know the laws that apply to themselves. The Foreign Intelligence Surveillance Court (FISC) was created in 1978 as a compromise, that generalist federal judges would oversee issuance of foreign intelligence orders but keep the orders secret to protect national security.

The risk of secret law became more acute after 2001, as the FISC faced the question of whether entire programs, such as Section 215 telephone meta-data, PRISM, and Upstream, were being carried out in compliance with statutory provisions. In calling for greater transparency, PCLOB's 215 report urged that, to the maximum extent consistent with national security, the government create and release with minimal redactions declassified versions of new decisions, orders and opinions by

[83] USA Freedom Act, Sec. 104, available at https://www.congress.gov/bill/114th-congress/house-bill/2048
[84] USA Freedom Act, Sec. 104.
[85] USA Freedom Act, Sec. 103.
[86] USA Freedom Act, Sec. 201.
[87] USA Freedom Act, Sec. 501.
[88] The program ended in November 2015.

the FISC in cases involving novel interpretations of FISA or other significant questions of law, technology or compliance.

Action: Although significant opinions of the FISC had always been provided to congressional oversight committees, the Obama administration began systematic declassification of FISC opinions, for the first time, in 2013. The stated goal was to carefully review each opinion, and disclose the actions of the FISC to the extent possible. By February 2015, the intelligence community had posted more than 250 declassified documents comprising more than 4,500 pages. Many of these documents related to proceedings of the FISC.[89]

The USA Freedom Act codified this effort.[90] From now on, the government will review each decision, order, and opinion of the FISC or the court that reviews it that includes "a significant construction or interpretation of any provision of this Act." After the review, the full or redacted opinion shall be made publicly available "to the greatest extent practicable." If a court action cannot be made public due to national security, the government must summarize "the significant construction or interpretation" of the legal provision.[91]

(7) Appointment of experts to brief the FISC on privacy and civil liberties.

Issue: When the FISC was created in 1978, its principal task was to decide whether a phone wiretap for one individual met the statutory standard. This task is essentially the same as a judge deciding to issue a warrant or other court order for a traditional law enforcement case. Under US law, such orders are issued *ex parte*, that is, the government presents its evidence and the court makes its decision, without representation from the criminal defendant.

After 2001, along with these individual orders, the FISC was faced with the decision whether to issue court orders for entire surveillance programs, such as Section 215 phone meta-data, Section 702 PRISM, and Section 702 Upstream. In my view, the FISC was acting somewhat similarly to a regulatory agency – is this overall program operating under the correct procedures and safeguards? Under US law, regulatory decisions of this magnitude generally occur only after a judge has received briefing from one or more non-government viewpoints. Both the Review Group and the PCLOB recommended that a panel of advocates be appointed so that the FISC would hear independent views on novel and significant matters.

[89] http://icontherecord.tumblr.com/ppd-28/2015/enhancing-transparency www.icontherecord.tumblr.com

[90] The newly re-issued Intelligence Community Directive on the National Intelligence Priorities Framework, ICD 204, codifies some of these issues. http://fas.org/irp/dni/icd/icd-204.pdf

[91] USA Freedom Act, Sec. 602.

Action: The USA Freedom Act authorized the creation of a group of independent experts, called "amicus curiae" (friend of the Court), to brief the FISC on important cases.[92] The law instructs the FISC to appoint an amicus curiae for a matter that, in the opinion of the court, "presents a novel or significant interpretation of the law." The court retains some discretion on when to appoint an amicus curiae, but the clear intent of the statute is that independent lawyers with security clearances shall participate before the FISC in important cases.

This reform provides the opportunity for independent views to be heard by the FISC for important cases, so that the assertions of government officials can be carefully tested before the judge. The statute does not precisely state what role the amicus curiae should play, but the first criterion for selection is "expertise in privacy and civil liberties." The FISC has named five expert lawyers, including Professor of Law Laura Donohue of Georgetown University, who has written extensively on civil liberties and foreign intelligence law, as well as lawyers who have been involved in these matters either in prior government service or in private practice.[93]

(8) Transparency Reports by Companies Subject to Court Orders

Issue: As discussed in Chapter 1, transparency is a central component of governing secret intelligence agencies in an open democracy. Historically, the companies who receive national security-related requests have been under strict limits about what they could disclose. For instance, companies could not even confirm or deny whether they had ever received a National Security Letter. In the absence of information about the scope of requests, skeptical people outside of the intelligence agencies feared "mass and indiscriminate surveillance." Both the Review Group and the PCLOB recommended that the government work with Internet service providers and other companies that regularly receive FISC orders to develop rules permitting the companies to voluntarily disclose more detailed statistical information concerning those orders.

Action: In 2014, the US Department of Justice reached agreement with major service providers (e.g., webmail and social network providers) that they could disclose considerably more detailed and extensive information about national security requests. Going forward, these service providers could publish these details in the annual or semi-annual Transparency Reports that a growing range of companies have released in recent years.

Consistent with the 2014 agreement, the USA Freedom Act guaranteed the right of those subject to national security orders to publish detailed statistics.[94] The

[92] USA_Freedom Act, Sec. 401.
[93] http://www.fisc.uscourts.gov. For a recent report on how one such amicus curiae case hs worked in practice, see https://www.techdirt.com/articles/20151210/08175733048/fisa-courts-appointed-advocate-not-allowing-governments-national-security-assertions-to-go-unchallenged.shtml]
[94] USA Freedom Act, Sec. 604.

companies can report statistics in a number of categories, such as content, non-content, and National Security Letters. Notably, the companies can report "the total number of all national security process received," including National Security Letters and orders under FISA. They can also report "the total number of customer selectors targeted under all national security process received."

In my view, these statistics provide important evidence about the actual scope of national security investigations in the United States. The percentage of users whose records are accessed in the most recent six-month period is vanishingly small. I have examined the most recent transparency reports of Facebook and Google, because European privacy regulators have focused particular attention on them in recent years. These statistics show what accounts have been accessed in the United States – the precise European concern about how individual data is handled once it leaves Europe and goes to the US. The statistics show far more targeted activity than the speculation in the popular press.[95]

Of the six categories reported, the highest percentage of users affected is for content requests to Google, a maximum of .0014%, or about 1 in 100,000. In total, the number of customer accounts accessed by the US government for national security in the most recent time period is approximately 10,000[96] for Facebook, out of approximately 1.55 billion[97] active users per month. The number of customer accounts accessed is approximately 17,000[98] for Google, out of approximately 1.17 billion[99] active users per month.

---

[95] My understanding is that the company transparency reports clearly cover the PRISM program, where specific selectors are made available to service providers such as Facebook and Google under the law. I do not know whether the statistics also include any government access under the Upstream program, where the government may gain access to an email, for example, without directly requesting that information from the email service provider. In terms of overall volume, however, it is relevant to consider Chapter 2, which discussed the declassified FISC opinion in 2011 that over 90 percent of the electronic communications acquired under Section 702 came from the PRISM program rather than the Upstream program. Even if Upstream statistics are not included in the transparency reports, that would shift one of the statistics here from roughly 1 in 1 million subscribers to 1 in 900,000 subscribers. The main point would remain the same – a vanishingly small fraction of users' communications are actually acquired by the NSA.

[96] For the most recent reporting period, companies were permitted to report aggregate numbers of requests received, during a six-month time period, from the government for intelligence purposes; the number of requests are reported in increments of 1,000. For the time period from July – December 2014, Facebook received the following: 0-999 non-content requests; 7,000-7,999 content requests; and 0-999 national security letters. https://govtrequests.facebook.com/country/United%20States/2014-H2/

[97] http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[98] For the time period from January – June 2014, Google received the following: 0-999 non-content requests; 15,000-15,999 content requests; and 0-999 national security letters, available at https://www.google.com/transparencyreport/userdatarequests/US/

[99] http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts

Facebook	# of Users Accessed in 6 months	Percentage based on Users Per Month
Non-Content Requests	0-999	.00006 %
Content Requests	7,000-7,999	.00052%
National Security Letters	0-999	.00006%

Google	# of Users Accessed in 6 months	Percentage based on Users Per Month
Non-Content Requests	0-999	.00009%
Content Requests	15,000-15,999	.00137%
National Security Letters	0-999	.00009%

These statistics put in perspective concerns that US intelligence agencies are massively accessing the information held by US service providers when data is transferred to the US. Both Facebook and Google are widely used in the EU. Based on the public reports, a maximum of 1 in 100,000 users has his or her content accessed in a six-month period, with other categories of request considerably lower. For the less-used categories, such as non-content requests to Facebook, that figure is approximately 1 in 1 million users – one person in a city of one million people.

(9) Transparency Reports by the US Government

Issue: the government has access to the classified information about national security investigations, and so is in the best position to report accurately to Congress and the public. FISA in 1978 established some reporting to the public, particularly the number of orders issued and the number denied. Congress, through the Senate and House Intelligence Committees, received more detailed reports and conducted classified oversight investigations into intelligence community activities. The required transparency reports, however, had not been updated after 2001 to reflect the broader set of intelligence and national security activities.

Action: The USA-Freedom overhauled the annual reporting by the US government about its national security investigations.[100] Going forward, the government each year will report statistics publicly for each category of investigation. For instance, for Section 702, the government will report the total number of orders as well as the estimated number of targets affected by such orders. The plain language of the statute thus provides that the US government will report annually on how many total targets have been affected by the PRISM and upstream collection programs. This level of transparency is remarkable for the actions of secret intelligence agencies. As with the transparency reports by companies, European officials and the general public can thus know the magnitude of these surveillance programs and changes in size over tune, rebutting in my view the claim of "mass and unrestrained surveillance."

[100] USA-Freedom, Sec. 603.

(10) Imminent passage of the Judicial Redress Act

Issue: The Privacy Act of 1974 provides a number of data protection measures that apply to "US persons" – US citizens and permanent residents. For a number of years, European data protection authorities and other officials have made reform of the Privacy Act a priority in trans-Atlantic privacy discussions. For instance, the issue was highlighted by the European Commission and members of the European Parliament when they briefed the Review Group in 2013. The basic request has been to provide the same protections to EU citizens as applied to US persons.

Action: The US government took steps before 2013 to provide Privacy Act protections in important respects. For instance, in 2007 the Department of Homeland Security applied the Privacy Act to "mixed" systems of records (databases that contain both US persons and non-US persons) to the extent permitted by law.[101] The current version of the Privacy Act, however, does not enable an agency to provide an appeal from an agency action to a judge, and this has been a concern to European officials.

The Judicial Redress Act has been moving through Congress to address this topic.[102] In EU/US negotiations related to privacy, passage of the Judicial Redress Act has become important both for discussions of a revised Safe Harbor agreement and for the "Umbrella Agreement" concerning law enforcement information to go into full effect.[103]

The Judicial Redress Act[104] passed the House of Representatives in October 2015 with bipartisan support, on a voice vote. The bill is now being considered by the Senate. My hope and belief is that the bill will pass the Senate, in which case President Obama would sign it into law.[105]

C. Executive Branch Actions

As discussed in the section on legislation, the executive branch was the first to take a number of actions that were subsequently codified into law by Congressional action. This part of the Chapter focuses on the numerous other executive branch actions since June, 2013. Many of these actions are summarized in "Signals Intelligence Reform: 2015 Anniversary Report,"[106] which was published near the one-year anniversary of President Obama's major speech on intelligence

---

[101] Department of Homeland Security: Privacy Policy Guidance Memorandum No. 2007-1 (January 7, 2007) (amended on January 19, 2007), available at Department of Homeland Security: Privacy Policy Guidance Memorandum No. 2007-1 (January 7, 2007)

[102] https://www.congress.gov/bill/114th-congress/house-bill/1428

[103] http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm

[104] https://www.govtrack.us/congress/bills/114/hr1428

[105] Predictions about what will pass the Congress are necessarily uncertain. I am offering my personal estimation that the bill will likely pass the Senate in the coming months.

[106] http://icontherecord.tumblr.com/ppd-28/2015/factsheet

reform.[107] A similar report is due to be published in January, 2016. Those interested in US surveillance practice and reform should refer to that report when it is issued.

The discussion here begins with broad conceptual reforms to US signals intelligence (SIGINT) that President Obama announced in 2014, and then examines the multiple other actions since 2013.

Issue: Historical practice, for the US and other nations, has been to provide greater latitude for surveillance outside of the country than within the country. Simply put, nations have spied on each other since Sun Tzu's classic *The Art of War* in ancient China, and well before that.[108] That is consistent with the Intelligence Community's mission to conduct foreign intelligence activities. Spying on hostile actors is especially understandable during time of war or when there is reason to believe hostile actors may attack.

The United States and the member states of the European Union have a shared legal tradition and strong alliances. Many in the EU have strongly objected to the scope of US surveillance reported since 2013. One way to understand the objections is that Europeans believe that EU citizens deserve similar treatment to US citizens when it comes to US surveillance activities. The longstanding international practice – the greater latitude to spy on non-citizens outside of one's own country – is, as applied to Europeans, contrary to the views of many in Europe about what is proper today for an ally such as the US.

Action: In 2014 President Obama issued Presidential Policy Directive-28 (PPD-28),[109] which I consider a historic document. Binding on all US intelligence agencies for their signals intelligence activities, the directive: "articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes." PPD-28 sets forth a number of new and distinct policies, with key items featured here.[110] In short, PPD-28 makes protecting the privacy and civil liberties rights of persons outside the US an integral part of US surveillance policy, and a direct order from the President, who is also Commander in Chief.[111]

---

[107] https://www.whitehouse.gov/blog/2014/01/17/president-obama-discusses-us-intelligence-programs-department-justice

[108] For a translation of the chapter on spies in *The Art of* War, see http://suntzusaid.com/book/13.

[109] https://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf

[110] An Interim Progress Report on Implementing PPD-28 was released in October 2014, available at http://icontherecord.tumblr.com/post/100240011473/interim-progress-report-on-implementing-ppd-28. Additional information is included in the 2015 Anniversary Report, at http://icontherecord.tumblr.com/post/100240011473/interim-progress-report-on-implementing-ppd-28.

[111] As with any other US Executive Order or Presidential Policy Directive, the President's announcement cannot create a right of action enforceable in court. Based on my experience in the US government, however, agencies go to great lengths to comply with directives from the President of

(11) New surveillance principle to protect privacy rights outside of the US

Issue: Longstanding law and practice in the US (and all other nations of which I am aware that follow the rule of law) is that greater legal protections are provided within a nation's borders than for surveillance conducted outside the borders.

Action: PPD-28 announced a new principle that applies to all intelligence agencies in the US when conducting signals intelligence: "Our 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, and that all persons have legitimate privacy interests in the handling of their personal information." It adds: "Privacy and civil liberties shall be integral considerations in the planning of US signals intelligence activities." I am not aware of any other country having announced and adopted principles of this sort in their intelligence activities.

(12) Protection of civil liberties in addition to privacy

Issue: The EU treats privacy as a fundamental right, among other fundamental rights such as freedom of expression.

Action: PPD-28 protects civil liberties as well as privacy: "The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion." PPD-28 clearly states that signals intelligence must be based on a legitimate purpose: "Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes."

(13) Safeguards for the personal information of all individuals, regardless of nationality

Issue: For the general principle of protecting privacy rights to matter in practice, it must be built into the operations of the agencies.

Action: Section 4 of PPD-28 sets forth detailed safeguards for handling personal information. It instructs each agency to establish policies and procedures, and to publish them to extent consistent with classification requirements. By 2015, all intelligence agencies had completed new policies or revised existing policies to meet the President's mandates.[112] The policies and procedures address topics

---

the United States. The PPD is binding upon executive branch agencies as an instruction from the head of the executive branch, even if it cannot be enforced by outsiders.

[112] The NSA policies and procedures to protect personal information collected through SIGINT can be found at: https://www.nsa.gov/public_info/_files/nsacss_policies/PPD-28.pdf Links to the policies

including: data security and access; data quality; and oversight, and "to the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

One of the over-arching principles of PPD-28 is minimization, an important issue often mentioned by EU data protection experts. The new safeguards in PPD-28 include: "Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized." This quotation does not mention words from EU data protection law such as "necessary" and "proportionate," but being "as tailored as feasible" and prioritizing alternatives to signals intelligence are two of many examples in US law where specific safeguards address those concerns.

(14) Retention and dissemination limits for non-US persons similar to US persons

Issue: A frequent concern expressed by European data protection officials is that stricter rules apply to US persons than to non-US persons, such as for the retention and dissemination of personal data.

Action: The agency procedures put in place pursuant to Section 4 of PPD-28 have created new limits that address this concern.[113] The new retention requirements and dissemination limitations are consistent across agencies and similar to those for US persons.[114] For retention, different intelligence agencies had previously had different rules for how long information about non-US persons could be retained. Under the new procedures, agencies generally must delete non-US person information collected through signals intelligence five years after collection.[115] For dissemination, there is an important provision applying to non-US persons collected outside of the US: "personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted."

---

and procedures for the ODNI, the CIA, the FBI, and other agencies can be found at: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties
Additional policies on the site include: National Reconnaissance Office, Department of Homeland Security, Drug Enforcement Administration, State Department, Treasury Department, Department of Energy, US Coast Guard, and Other IC Elements in the Department of Defense.

[113] The US government will not consider the activities of foreign persons to be foreign intelligence just because they are foreign persons; there must be some other valid foreign intelligence purpose.

[114] The agency procedures create new limits on dissemination of information about non-US persons, and require training in these requirements.

[115] There are exceptions to the five-year limit, but they can only apply after the Director of National Intelligence considers the views of Office of the Director of National Intelligence Civil Liberties Protection officer and agency privacy and civil liberties officials. http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties

The agency procedures make other changes for protection of non-US persons, including new oversight, training, and compliance requirements: "The oversight program includes a new requirement to report any significant compliance incident involving personal information, regardless of the person's nationality, to the Director of National Intelligence."[116]

(15) Limits on bulk collection of signals intelligence

Issue: In the wake of the Snowden revelations, there has been particular concern about bulk collection by US intelligence agencies.

Action: Section 2 of PPD-28 creates new limitations on the use of signals intelligence collected in bulk, where "bulk" is defined as "authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants," such as the email or other selectors discussed in Chapter 2.[117]

PPD-28 announces purpose limitations -- when the US collects nonpublicly available information in bulk, it shall use that data only for purposes of detecting and countering:

1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
2) Threats to the United States and its interests from terrorism;
3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction;
4) Cybersecurity threats;
5) Threats to U.S. or allied Armed Forces or other U.S or allied personnel;
6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.

If this is updated, it will be "made publicly available to the maximum extent feasible."

(16) Limits on surveillance to gain trade secrets for commercial advantage

Issue: European and other nations have long expressed concern that US surveillance capabilities would be used for the advantage of US commercial interests. These

[116] http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28

[117] Consistent with the discussion if filtering in Chapter 2, PPD-28 says: "The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection." The detailed rules governing targeted collection under Section 702 are discussed in Chapter 2.

concerns, if true, would provide an economic reason to object to US signals intelligence, in addition to privacy and civil liberties concerns.

Action: The Review Group was briefed on this issue, and we reported that US practice has *not* been to gain trade secrets for commercial advantage. There is a subtlety here that is sometimes overlooked. PPD-28 states that the "collection of foreign private commercial information or trade secrets is authorized," but only "to protect the national security of the United States or its partners and allies." For instance, the national security of the US and its EU allies justifies surveillance of companies in some circumstances, such as evading sanctions and shipping nuclear materials to Iran, or money laundering to support international terrorism.

The distinction in PPD-28 is that "It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially." In the above examples, it would not be justified to collect information for the purpose of assisting a US nuclear equipment manufacturer or US banks.

(17) New White House oversight of sensitive intelligence collection, including of foreign leaders

Issue: In the aftermath of the attacks of September 11, 2001, the view of intelligence agencies was that they had a tendency to conduct surveillance activities to collect foreign intelligence information against a wide range of targets, without necessarily taking into account non-intelligence consequences of that targeting.

Action: To review sensitive intelligence collection more closely, there is now a stricter procedure to assess sensitive intelligence collection, as part of the National Intelligence Priorities Framework.[118] The procedures have been revised to require more senior policymaker participation in collection decisions. In the first year, the new procedures applied to nearly one hundred countries and organizations, resulting in new collection restrictions.[119] In addition, the NSA "has enhanced its processes to ensure that targets are regularly reviewed, and those targets that are no longer providing valuable intelligence information in support of these senior policy-maker approved priorities are removed."[120]

The new oversight process responds in part to the new principles of respecting privacy and civil liberties abroad. The rationale for careful oversight is bolstered by heightened awareness that "US intelligence collection activities present the potential for national security damage if improperly disclosed."[121] Potential

[118] http://icontherecord.tumblr.com/ppd-28/2015/limiting-sigint-collection
[119] Id.
[120] Id.
[121] PPD-28, Sec. 3

damage cited in PPD-28 includes compromise of intelligence sources and methods, as well as harm to diplomatic relationships and other interests.

This process includes review of collection efforts targeted at foreign leaders. For many observers, it is reasonable for the US or another country to seek to monitor the communications of foreign leaders in time of war or concerning clearly hostile nations. By contrast, the US was widely criticized for reported efforts to monitor the communications of German Chancellor Angela Merkel and the leaders of other allied countries. Collection targeted at foreign leaders is now reviewed as part of the overall White House oversight of sensitive intelligence collection.. President Obama stated in 2014: "I have made clear to the intelligence community that unless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies."[122]

(18) New White House process to help fix software flaws rather than use them for surveillance

Issue: The Review Group recommended a new process to evaluate what to do with so-called "Zero Day" attacks, where software developers and system owners have zero days to address and patch the vulnerability.[123] The Review Group recommended that the government should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are quickly patched on government and private networks.

Action: Previously, the decision was made in the NSA about how to balance the equities between the usefulness of a Zero Day for offense (to penetrate someone else's network for surveillance) vs. for defense (to patch our own networks). In 2014 the White House announced what it called a "disciplined, rigorous and high-level decision-making process for vulnerability disclosure."[124] In my view, this new inter-agency process, chaired by the President's Cybersecurity Coordinator, improves on the old system by bringing in perspectives from more stakeholders who emphasize the importance of defending networks. In other words, the new process creates a new and useful check on any intelligence agency temptation to emphasize surveillance capabilities at the expense of good cybersecurity and protection of the personal data in computer systems.

(19) Greater transparency by the executive branch about surveillance activities

---

[122] https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[123] Review Group Report, at 219.

[124] https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

Issue: Item 10 in this Chapter discussed new government transparency reports required in the USA Freedom Act.

Action: Since 2013, the executive branch has gone well beyond these legislative requirements in its transparency activities. In its January 2015 report on Signals Intelligence Reform, the government reported eight categories of greater transparency that it had undertaken to that point, and I expect additional items to be listed in the next report in January 2016.[125] Compared to the secrecy that historically had applied to signals intelligence, the shift toward greater transparency is remarkable, such as:

- The already-mentioned declassification of numerous FISC decisions;
- A new website devoted to public access to intelligence community information;[126]
- The first "Principles of Intelligence Transparency for the Intelligence Community;[127]
- The first two Intelligence Community Statistical Transparency Reports;[128]
- Unclassified reports on NSA's implementation of Section 702[129] and its "Civil Liberties and Privacy Protections for Targeted SIGINT Activities;[130] and
- Numerous speeches and appearances by intelligence community leadership to explain government activities, in contrast to the historical practice of very little public discussion of these issues.[131]

(20) Creation of the first NSA Civil Liberties and Privacy Office

Issue: In a 2013 talk, President Obama said: "Just because we can do something, doesn't mean we should do it."[132] The NSA staffed up its already significant compliance efforts after FISC criticism of its implementation of programs under FISA, including hiring a Director of Compliance, and now has over 300 compliance employees.[133] Simply complying with law, however, does not mean that there is sufficient attention to how privacy should be treated within an intelligence agency.

---

[125] http://icontherecord.tumblr.com/ppd-28/2015/enhancing-transparency
[126] http://icontherecord.tumblr.com
[127] http://www.dni.gov/files/documents/ppd-28/FINAL%20Transparency_poster%20v1.pdf http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf
[128] http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014
[129] https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf
[130] https://www.nsa.gov/civil_liberties/_files/nsa_clpo_report_targeted_EO12333.pdf
[131] http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014
[132] http://www.politico.com/story/2013/10/obama-surveillance-message-lost-in-translation-099003#ixzz3uLEoiGaW
[133] https://www.nsa.gov/civil_liberties/_files/nsa_clpo_report_targeted_EO12333.pdf

Action: NSA appointed a Civil Liberties and Privacy Officer for the first time,[134] and other agencies have similar positions.[135] That office becomes a point of expertise within the agency, and a point of contact for those outside of the agency who have privacy concerns.[136]

(21) Multiple changes under Section 215

Issue: In his 2014 speech, President Obama ordered multiple changes to the bulk telephony metadata program conducted under Section 215.[137]

Action: In response, the executive branch changed its practices under Section 215 in numerous ways.[138] Congress faced a "sunset" of the Section 215 authority in 2015 – if Congress did not act, then the legal authority as it currently existed would have expired. The existence of this sunset created a powerful incentive for Congress to consider the USA Freedom Act, which extended Section 215 with the numerous pro-privacy changes described earlier in this chapter.

(22) Stricter documentation of the foreign intelligence basis for targeting under Section 702

Issue: A prominent criticism of US surveillance law has been that it constitutes "indiscriminate" surveillance, including under the PRISM and upstream programs of Section 702. Under the OECD Privacy Guidelines[139] and EU data protection law, there should be a clear purpose specification for the processing of personal data. While collection under Section 702 has always been targeted rather than indiscriminate, the executive branch has instituted measures to ensure that the targeting is appropriately documented.

---

[134] President Obama issued PPD-28 on January 17, 2014. http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#section-215
The US government announced NSA's first CLPO on January 29, 2014. http://icontherecord.tumblr.com/tagged/becky+richards

[135] Sec 4(c).

[136] The Office of Director of National Intelligence similarly has a Civil Liberties Protection Officer, www.dni.gov/clpo. Other relevant agency positions include: Department of Homeland Security Privacy Officer, http://www.dhs.gov/privacy-office,: Department of Homeland Security Office for Civil Rights and Civil Liberties - http://www.dhs.gov/office-civil-rights-and-civil-liberties.: Department of Justice Office of Privacy and Civil Liberties http://www.justice.gov/opcl.; Department of Defense Oversight and Compliance Directorate http://dcmo.defense.gov/About/Organization/OCD.aspx, which includes the Defense Privacy and Civil Liberties Office http://dpcld.defense.gov/ and Department of Defense Intelligence Oversight http://dodsioo.defense.gov/Home.aspx.

[137] https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[138] "New privacy protections for bulk telephony metadata collected under Section 215," http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#section-215

[139] http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Action: In its detailed report on Section 702 in 2014, the first recommendation by the PCLOB was to "Revise NSA Procedures to Better Document the Foreign Intelligence Reason for Targeting Decisions."[140] In 2015, the PCLOB reported: "The Administration has agreed to implement this recommendation."[141]

The PCLOB's 2015 assessment provides details about the change, including:

- Revision of the NSA's targeting procedures to specify criteria for determining the expected foreign intelligence value of a particular target;
- Further revision to require a detailed written explanation of the basis for the determination;
- FISC review of the revised targeting procedures and requirements of documentation of the foreign intelligence finding;
- Other measures to ensure that the "foreign intelligence purpose" requirement in Section 702 is carefully met;
- Submission of the draft targeting procedures for review by the PCLOB (an independent agency with privacy responsibilities); and
- Compliance, training, and audit.[142]

(23) Other changes under Section 702

Issue: Chapter 2 of this testimony discussed in detail Section 702's PRISM and upstream programs. Section 702 sunsets in 2017, so Congress will face a similar debate to the one in 2015 for Section 215.

Action: The PCLOB issued a lengthy report on Section 702 in 2014, which included recommendations for reform by the executive branch.[143] In 2015, the PCLOB assessed the government's response: "The Administration has accepted virtually all of the recommendations in the Board's Section 702 report and has begun implementing many of them."[144] A number of the recommendations apply to US persons and thus are not the focus here.

In addition to the new requirements for purpose specifications, the detailed assessment by the PCLOB included the following:[145]

- Provide the FISC random samples of selectors used for targeting under the Section 702 program, to enhance the court's review of the overall program. As of the time of the report, this was being implemented.

---

[140] https://www.pclob.gov/library/702-Report.pdf
[141] https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf
[142] PPD-28's Section 2 also provides guidance for clearer purpose specification in connection with bulk collection.
[143] https://www.pclob.gov/library/702-Report.pdf
[144] https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf
[145] A number of the recommendations apply to US persons and thus are not the focus here.

- Provide the FISC with consolidated documentation about Section 702. According to the PCLOB, the program had become so complex that this documentation was necessary. As of the time of the report, this was being implemented.
- Periodically assess upstream collection technology to ensure that only authorized communications are required. The administration has accepted this recommendation.
- Examine the technical feasibility of limiting particular forms of "about" information. "About" information was discussed in Chapter 2 of this testimony. The NSA has been assessing how to achieve greater minimization of "about" information.
- Publicly release the current Section 702 minimization procedures for the CIA, FBI, and NSA. This has been done.

(24) Reduced secrecy about National Security Letters

Issue: As enacted in 2001, recipients of a National Security Letter were "gagged" – they were not allowed to tell anyone that they had received the NSL.[146] In law enforcement investigations, recipients of a wiretap order are similarly prohibited from telling the target about the wiretap, for obvious reasons – targets will not say incriminating things if they know the police are listening. Within weeks or at most months of the end of the investigation, however, targets are informed about the wiretap. For NSLs, however, the prohibition on disclosure continued indefinitely.[147]

Action: In his 2014 speech, President Obama announced the indefinite secrecy would change. As of 2015, the FBI will now presumptively terminate NSL secrecy for an individual order when an investigation closes, or no more than three years after the opening of a full investigation. Exceptions are permitted only if a senior official determines that national security requires otherwise in the particular case and explains the basis in writing.[148]

D. Conclusion

Since the first press disclosures from Snowden approximately 30 months ago, the US government has taken the two dozen actions discussed in this chapter. As this chapter has shown, these reforms emerged from a transparent and extensive process, including extensive debate in the US Congress and hundreds of pages of expert reports and declassified intelligence documents.

---

[146] I first wrote about problems with this gag rule in 2004. Peter Swire, "The System of Foreign Intelligence Surveillance Law," 72 *Geo. Wash. L. Rev.* 1306 (2004), available at http://ssrn.com/abstract=586616.

[147] The statistical number of NSLs received can be reported in increments of 1000 by providers, as discussed above concerning government transparency reports.

[148] http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties

These reforms were not mentioned in the European Court of Justice decision in *Schrems*, or in the Opinion of the Advocate General, despite the latter's statement that assessment of US practices must be done "by reference to the current factual and legal context."

The reforms show the nature of the US "legal order" relating to surveillance activities. They show a constitutional democracy under the rule of law, with independent judicial oversight, transparency, and democratic accountability. As discussed in Chapter 1, they show the essential and fundamental equivalence of the US and EU member states with respect to surveillance activities.

- / -

Peter Swire is the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business and a Senior Fellow of the Future of Privacy Forum. He is Senior Counsel with the law firm of Alston & Bird, LLP; nothing in this document should be attributed to any client of the firm.

Swire has long worked on both EU data protection law and US surveillance law. In 1998, he was lead author of the book "None of Your Business: World Data Flows, E-Commerce, and the European Privacy Directive." He was Chief Counselor for Privacy in the U.S. Office of Management and Budget during negotiation of the Safe Harbor agreement. While in that position, he chaired a White House working group on how to update U.S. wiretap laws for the Internet. He was one of five members of President Obama's Review Group on Intelligence and Communications Technology (the "NSA Review Group"), whose 2013 report has been republished by the Princeton University Press.

Swire thanks DeBrae Kennedy-Mayo, Research Associate at the Georgia Tech Scheller College of Business, for her work on this paper. Further publications and information at www.peterswire.net. For corrections or comments, please email to peter.swire@scheller.gatech.edu.

The Future of Privacy Forum (FPF) is a Washington, DC based think tank that seeks to advance responsible data practices. The forum is led by Internet privacy experts Jules Polonetsky and Christopher Wolf and includes an advisory board comprised of leading figures from industry, academia, law and advocacy groups.