CHAPTER 3:

SYSTEMIC SAFEGUARDS IN THE US SYSTEM OF FOREIGN INTELLIGENCE SURVEILLANCE LAW

[1] This Chapter describes the systemic safeguards that exist in the US against abuse in the foreign intelligence surveillance area. The US government is founded on the principle of checks and balances against excessive power. The risk of abuse is potentially great for secret intelligence agencies in an open and democratic society – those in power can seek to entrench themselves in power by using surveillance against their enemies. The US experienced this problem in the 1970s, when the Watergate break-in occurred against the opposition political party, the Democratic Party national headquarters. In response, the US enacted numerous safeguards against abuse, including the Foreign Intelligence Surveillance Act of 1978 (FISA). In recent years, following the Snowden revelations that began in 2013, the US has enacted an extensive set of additional safeguards against excessive surveillance, as shown by the list of two dozen reforms discussed in my 2015 testimony for European privacy regulators, and by additional safeguards put in place this year as well.

[2] As discussed in Chapter 2, I published the lengthy law review article "The System of Foreign Intelligence Surveillance Law" in 2004.[1] Based on my experience in government, interviews with leading experts, and academic research, this article emphasized the *system* of checks and balances against abuse. Foreign intelligence surveillance typically involves highly classified information about other nations and their agents, so there are large risks to the nation's foreign relations and national security if details about the surveillance are made public. As discussed in Chapter 8, I therefore believe that individual remedies for foreign surveillance issues are often ill-advised – they create a vector of attack for hostile actors to learn the details of the top secret information. Courts in the US and EU have recognized the importance of keeping these state secrets from being disclosed in open court.

[3] Because individual remedies play a limited role for foreign intelligence surveillance, the fundamental safeguards against abuse are at the systemic level. This basic reliance on system-wide safeguards is familiar in many settings. For instance, we have company-wide audits of the finances of the typical company. The auditors check the financial systems in a thorough way. On occasion, there may be individual remedies, where an investor or someone else believes there was a problem and perhaps files a lawsuit. The main protection against fraud and mistake in most instances, however, comes from the systemic audits, not the occasional individual complaint. Even where there is a complaint, furthermore, the issue often gets resolved by review of the audit logs rather than public disclosure in court of detailed and confidential business information.

[4] Applied to foreign intelligence surveillance, the US approach has been to create a large set of statutory safeguards, supplemented by administrative safeguards and multiple oversight mechanisms as well as transparency when feasible. This Chapter describes these safeguards in detail. It documents the large compliance system developed over time at the National Security Agency (NSA), and the findings of outside reviewers that the NSA operating under current law has been focused on its national security mission, and has not been targeting political opponents' behavior.

[5] At the same time, I note that the numerous individual remedies US law provides in addition to systemic protections – discussed in detail in Chapter 7 – can have system-wide impacts that complement the safeguards outlined in this Chapter. As an example, Chapter 7 discusses a

[1] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004), http://peterswire.net/wp-content/uploads/Swire-the-System-of-Foreign-Intelligence-Surveillance-Law.pdf.

criminal remedy within the US Foreign Intelligence Surveillance Act that makes it a crime to conduct unauthorized surveillance.[2] When compliance incidents have arisen, the Foreign Intelligence Surveillance Court has indicated its intent to investigate whether individuals in intelligence agencies committed such a crime.[3] This has resulted in, for example, the NSA deciding to delete all data that one of its surveillance programs collected prior to October of 2011.[4] Another individual remedy with systemic ramifications is the right of criminal defendants to exclude evidence obtained by unlawful or unauthorized surveillance, thus making the government unable to use it in prosecutions.[5] The effects of these individual remedies can reverberate through foreign intelligence practice, reinforcing the US's system of safeguards this Chapter discusses.

[6] Section I of this Chapter provides historical background for the system of US foreign intelligence law, as well as the fundamental safeguards built into the US system of constitutional democracy under the rule of law. Section II describes the systemic statutory safeguards governing foreign intelligence surveillance. Section III describes the oversight mechanisms, and Section IV the transparency mechanisms. Section V describes administrative safeguards that are significant in practice and supplement the legislative safeguards. A separate Chapter, Chapter 5, then shows how these safeguards apply in a case study. That Chapter reports, based on review of court cases and other material declassified since 2013, how the Foreign Intelligence Surveillance Court (the FISC) has applied these safeguards in practice. Overall, in my view, there has been an impressive system of oversight for US foreign intelligence practices. As discussed in Chapter 6, I agree with the conclusion of a study led by an Oxford expert, Ian Brown, which found the US system has "much clearer rules on the authorization and limits on the collection, use, sharing, and oversight of data relating to foreign nationals than the equivalent laws of almost all EU Member States."[6] A central question of this case is whether the US has "adequate" safeguards around surveillance information; my review of the safeguards matches that of Professor Brown's – the US system generally has clearer and more extensive rules than the equivalent laws in Europe. In addition, the FISC case study shows how thoroughly those rules are implemented in practice in the US. There is no similar evidence, to the best of my knowledge, of anything like that level of protection in practice in the Member States.

I. The United States as a Constitutional Democracy under the Rule of Law

[7] My discussion of systemic safeguards begins with the most foundational safeguard – the history of the US as a constitutional democracy under the rule of law. I highlight four features of the US system of government: (1) a time-tested system of checks and balances; (2) judicial independence; (3) constitutional protection of individual rights; and (4) democratic accountability.

---

[2] *See* Chapter 7, Section I(B) (discussing 50 U.S.C. § 1809).

[3] *See* Chapter 5, Section II(B)(3)(E) (discussing how the Foreign Intelligence Surveillance Court indicated it intended to investigate whether the NSA committed a crime under 50 U.S.C. § 1809); *[Caption Redacted]*, [No. Redacted], 29-30 (F.I.S.C. Sept. 25, 2012), https://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.

[4] *See id.*

[5] For a more detailed discussion of exclusionary remedies, *see* Chapter 7, Section I(B). The US Classified Information Procedures Act further subjects the use of any classified information in criminal proceedings to supervision by an independent judge, while giving both the judge and defense access to the classified information. *See* Chapter 8, Section IV.

[6] Ian Brown et al., *Towards Multilateral Standards for Surveillance Reform*, 3 (2015), https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf.

This system of government has survived through more than two centuries of challenge and turmoil. No one would argue that every decision by every judge or leader has been correct; instead, the most fundamental assessment of "adequacy" or "essential equivalence" goes to whether the nation protects rights and freedoms under the rule of law.

[8] These four safeguards apply to the US foreign intelligence surveillance activities at the heart of Mr. Schrems' complaint. They also apply to US criminal procedure, which is explained in more detail in Chapter 4.

A. A Time-Tested System of Checks and Balances

[9] The US Constitution created a time-tested system of checks and balances among the three branches of government. The separation of powers among 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] The US Constitution provides detailed checks and balances among the three branches, as set forth in Article I (legislative branch), Article II (executive branch), and Article III (judicial branch).

[10] Compared with the EU Member States, the US Constitution has been in continuous operation since 1790, far longer than is true for most Member States. In contrast to some recently admitted Member States, where there have been questions about the effective protection of constitutional rights and the rule of law,[8] the US constitutional system of checks and balances has been enduring and remains in vigorous effect today.

B. Judicial Independence

[11] The judiciary is a separate branch of government in the US, established by Article III of the US Constitution. Federal judges are nominated by the President and confirmed by the Senate. The independence of federal judges is provided in the Constitution – appointments are for the lifetime of the judge, with removal only by impeachment, and with a guarantee of no diminution of salary.[9]

---

[7] "When the legislative and executive powers are united in the same person, or in the same body of magistrates, there can be no liberty; because apprehensions may arise, lest the same monarch or senate should enact tyrannical laws, to execute them in a tyrannical manner. Again, there is no liberty if the judiciary power be not separated from the legislative and executive. Were it joined with the legislative, the life and liberty of the subject would be exposed to arbitrary control [sic]; for the judge would be then the legislator. Were it joined to the executive power, the judge might behave with violence and oppression. There would be an end of every thing [sic], were the same man, or the same body, whether of the nobles or of the people, to exercise those three powers, that of enacting laws, that of executing the public resolutions, and of trying the causes of individuals." [1 THE SPIRIT OF LAWS], CHARLES LOUIS DE SECONDAT, BARON DE MONTESQUIEU, *Book XI Ch. VI – Of the Constitution of England*, COMPLETE WORKS, 198, 199, (1748), http://oll.libertyfund.org/titles/837.

[8] *See, e.g.*, EUROPEAN COMMISSION, *Rule of Law*, http://ec.europa.eu/justice/effective-justice/rule-of-law/index_en.htm (linking to European Parliament and European Commission resolutions and press releases surrounding concerns about Poland and Hungary).

[9] Article III, Section 1 of the US Constitution provides: "The judicial power of the United States, shall be vested in one Supreme Court, and in such inferior courts as the Congress may from time to time ordain and establish. The judges, both of the supreme and inferior courts, shall hold their offices during good behaviour, and shall, at stated

[12] European data protection law emphasizes the importance of an independent decision-maker to protect privacy rights.[10] The precise guarantees of judicial independence in EU Member States vary considerably.[11] The lifetime tenure and protection against diminution of salary provides a strong guarantee of the independence for US federal judges. This independence is important for the effectiveness of the Foreign Intelligence Surveillance Court, where decisions are all issued by such judges.

[13] Since the 1803 Supreme Court case of *Marbury v. Madison*, the judicial branch has the authority to engage in judicial review.[12] Judges have the legal power to strike down a statute that is contrary to the Constitution. For executive actions, judges have the legal power to issue binding orders to prevent the executive branch from violating either the US Constitution or applicable statutes.

C. Constitutional Protections of Individual Rights

[14] The US Constitution enumerates a set of rights that protect the individual against government action. As just mentioned, US judges have the power of judicial review. This power serves as a systemic check against abuse – a judge may strike down an entire statute or government program as unconstitutional. In addition, these rights protect individuals against unconstitutional action in a criminal prosecution – defendants can argue, for instance, that there was a violation of their rights under the Fourth Amendment (search and seizure) or First Amendment (free speech).

[15] For government access to personal data, the Fourth Amendment plays a particularly important role.[13] It states:

---

times, receive for their services, a compensation, which shall not be diminished during their continuance in office." U.S. CONST. art. 3, § 1.

[10] As the Article 29 Data Protection Working Party stated in its Privacy Shield Opinion: "The WP29 recalls that ideally, as has also been stated by the CJEU and the ECtHR, [surveillance] oversight should be in the hands of a judge in order to guarantee the independence and impartiality of the procedure." Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, 16/EN WP 238 at 41 (Apr. 13, 2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

[11] *See generally* European Commission for the Efficiency of Justice, *Study on the functioning of judicial systems in the EU Member States*, CEPEJ(2014)4final (Mar. 14, 2014), http://ec.europa.eu/justice/effective-justice/files/cepj_study_scoreboard_2014_en.pdf.

[12] 5 U.S. 137 (1803). US Supreme Court cases may be found at https://www.supremecourt.gov/opinions/opinions.aspx, or https://supreme.justia.com/.

[13] In my experience, there has been some confusion about the way that the Fourth Amendment applies to non-US persons, in the wake of *United States v. Verdugo-Urquidez*, 494 U.S. 1092 (1990). Briefly, the Fourth Amendment applies to searches and seizures that take place within the US (such as on data transferred to the US), and to searches against US persons (US citizens as well as permanent residents) that take place outside of the US. For foreign intelligence collected in the US, such as personal data transferred from the EU by a company, the Fourth Amendment continues to apply, because all searches must meet the overall Fourth Amendment test that they be "reasonable." *See In re Sealed Case*, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002). The EU Commission has recognized this rule: "While the Fourth Amendment rights does not extend to non-US persons that are not resident in the United States, the latter nevertheless benefit indirectly from its protections, given that the personal data are held by US companies with the effect that law enforcement authorities in any event have to seek judicial authorization (or at least respect the reasonableness requirement)." Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the

> 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.[14]

As I discussed in my 2015 testimony, the jurisprudence concerning the Fourth Amendment has responded to changing technology. Federal courts in recent years have issued a string of Fourth Amendment rulings to protect privacy, such as *Riley v. California* (warrant needed to search cell phones),[15] *United States v. Jones* (warrant needed when attaching a GPS device to a car),[16] *Kyllo v. United States* (warrant needed for high-technology search of home conducted from the street),[17] and *United States v. Warshak* (warrant needed to access email).[18] The probable cause requirement and other aspects of Fourth Amendment protection are discussed further below.

[16] Other constitutional protections for information about a person's information include:

- *First Amendment*. This amendment protects free speech, assembly, and association, providing a wide range of protections against government interference with freedom of thought and expression. With regards to privacy, the First Amendment protects a range of anonymous speech,[19] and protects the right of individuals to gather or communicate privately.[20]

- *Third Amendment*. Because soldiers had been quartered in homes during colonial times, the Founders specifically outlawed this practice under the Constitution. This protection supports the privacy of one's home.[21]

- *Fifth Amendment*. The prohibition on compelled self-incrimination protects the privacy of an individual's thoughts. In the context of electronic evidence, this provision of the US Constitution has been used to restrain the government from requiring an accused person from providing passwords and encryption keys.[22]

---

adequacy of the protection provided by the EU-U.S. Privacy Shield, para. 127, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL. For data that the US government collects in the US, statutory protections apply in addition to the Fourth Amendment, such as the Wiretap Act, 18 U.S.C. 119 §§ 2510-2522 and the Stored Communications Act, 18 U.S.C. 121 §§ 2701-2712.

[14] U.S. CONST. amend IV.

[15] 134 S. Ct. 2473 (2014).

[16] 565 U.S. 945 (2012) (holding a warrant is needed to install GPS device on a vehicle).

[17] 533 U.S. 27 (2001).

[18] 631 F.3d 266 (6th Cir. 2010), http://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf.

[19] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995).

[20] LEGAL INFORMATION INSTITUTE, *First Amendment: An Overview*, https://www.law.cornell.edu/wex/first_amendment.

[21] William Sutton Fields, *The Third Amendment: Constitutional Protection From the Involuntary Quartering of Soldiers*, 124 MIL. L. REV. 195 (Spring 1989).

[22] *See, e.g., In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, U.S. v. John Doe*, 670 F.3d 1335, 1352 (11th Cir. 2012), http://stanford.edu/~jmayer/law696/week8/Compelled%20Password%20Disclosure%20(Eleventh%20Circuit).pdf.

[17] These constitutional rights, enforced by independent judges, provide systemic protections against over-reach by the other branches of government.

D. Democratic Accountability

[18] Based on my study of US surveillance practices, I am impressed by the ability of the US as a democracy to correct for episodes of excessive surveillance. My 2004 article discussed in detail episodes in US history where civil liberties were not safeguarded as well as I believe they should be. The point I am making here is that, when excessive surveillance became known, the democratically-elected branches responded with new and significant safeguards.

[19] I highlight two examples, discussed in more detail below. The Watergate scandal under President Nixon was followed by a host of significant government reforms, including the Privacy Act of 1974, major expansion of the Freedom of Information Act in 1974, and the Foreign Intelligence Surveillance Act of 1978.[23] Following the Edward Snowden revelations that began in 2013, the US government undertook over two dozen significant surveillance reforms, including two notable statutes. The USA FREEDOM Act of 2015 created multiple new limits on foreign intelligence surveillance, and Congress also enacted the Judicial Redress Act in 2016,[24] as discussed in Chapter 7. These legislative safeguards, and accompanying administrative measures, are evidence of an ongoing political culture in the US that sets limits on surveillance powers, complementing the protection afforded by the US Constitution and the independent judiciary.[25]

II. Historical Context for Systemic Safeguards against Excessive Foreign Intelligence Surveillance

[20] Within the constitutional structure just discussed, today's systemic safeguards against excessive foreign intelligence surveillance are best understood as reflecting three periods: (1) the turbulent era of the 1960s and 1970s; (2) the reaction to the attacks of September 11, 2001; and (3) the period since the Snowden revelations began in 2013.

A. The 1960s and 1970s

[21] Major components of the current US system of safeguards come from the turbulent era of the 1960s and 1970s, from sources including the civil rights movement, Vietnam War protests, and the Watergate break-in.[26]

[22] In retrospect, I agree with leading scholars who see the civil rights movement as an important source for the protection in this period of individual constitutional rights by the US

---

[23] *See* Swire, *supra* note 1.

[24] Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2015), https://www.congress.gov/bill/114th-congress/house-bill/1428/text.

[25] Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, 32 Georgia Inst. Tech. Scheller College of Bus. Res. Paper No. 36 (Dec. 18, 2015), http://ssrn.com/abstract=2709619 [hereinafter *US Surveillance Law*]. This document was submitted as a White Paper to the Belgian Privacy Authority at its request for its Forum on "The Consequences of the Judgment in the Schrems Case."

[26] In my article on the system of foreign intelligence law, I discuss the history in some detail. Swire, *supra* note 1.

Supreme Court.[27] During the 1960s, the federal courts were deeply involved in cases such as school desegregation and addressing discrimination in employment, housing, and elsewhere. In what was sometimes called "massive resistance," state officials opposed federal court orders and acted in ways that federal courts increasingly held violated the constitutional rights of individuals. During this period, the Supreme Court increasingly applied federal constitutional protections against the actions of state officials. For instance, the Supreme Court held that evidence illegally obtained by police during a search cannot be used as evidence at trial.[28] It later held that the Fourth Amendment similarly prohibits information derived from illegal searches – the "fruit of the poisonous tree" – from being allowed into evidence.[29]

[23] As a notable example of this expansion of constitutional rights, the Supreme Court applied the Fourth Amendment to wiretaps and related electronic surveillance. In perhaps its most famous privacy-protective decision, *Katz v. United States*, the Supreme Court in 1967 held that the Fourth Amendment requires a judicially approved search warrant when doing a wiretap.[30] *Katz* announced a principle of individual fundamental rights – the Fourth Amendment applies outside of the home, and "protects people, not places."[31] In the same opinion, the Supreme Court recognized that national security wiretaps may raise special issues, without reaching a decision on how to govern such wiretaps.[32]

[24] 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.[33] In connection with Vietnam War protests, the defendant was charged with the dynamite bombing of an office of the US 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 within the discretion of the Executive Branch."[34] 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."[35]

---

[27] *See, e.g.*, MICHAEL KLARMAN, FROM JIM CROW TO CIVIL RIGHTS: THE SUPREME COURT AND THE STRUGGLE FOR RACIAL EQUALITY (2004).
[28] *Mapp v. Ohio*, 367 U.S. 643 (1961).
[29] *Wong Sun v. United States*, 371 U.S. 471, 488 (1963).
[30] 389 U.S. 347 (1967).
[31] *Id.* at 351.
[32] The Court wrote: "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." *Id.* at 358.
[33] *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297 (1972) [hereinafter "*Keith*"].
[34] *See* Trevor Morrison, *The Story of the United States v. United States District Court (Keith): The Surveillance Power*, Columbia Policy Law & Legal Theory Working Papers, No. 08155, 1 (2008), http://lsr.nellco.org/columbia_pllt/08155/ (quoting *Keith*, 407 U.S. at 316-17).
[35] 407 U.S. at 308. 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 the Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. 95–511, 92 Stat. 1783 (1978), https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (current version codified in scattered sections of 50 U.S.C.).

[25] The Watergate scandal triggered the next round of protections against excessive surveillance. The Watergate break-in itself was a burglary into the office of the opposing political party, exemplifying the risk that excessive surveillance can threaten political opponents, dissidents, or the democratic process itself. Indeed, in my opinion, the prevention of this sort of political abuse is quite likely the single strongest reason to support systemic safeguards against surveillance. Those in power have an incentive to entrench themselves in power, so we need a system of oversight, transparency, and checks and balances to fight back against such entrenchment. Such abuse was addressed by President Obama's Review Group on Intelligence and Communications Technology (Review Group), which is discussed further below and of which I was a member. One important finding of the Review Group was that we found no evidence of any such political abuses in our review of the US surveillance system. Although individuals may differ about what surveillance programs properly achieve both privacy and national security, it is comforting that our review at the top-secret level found the intelligence agencies focused on protecting national security, and not abusing their power for political or personal gain.

[26] As part of the investigations related to Watergate, the Church Commission and other inquiries found evidence of widespread, illegal surveillance by US intelligence agencies.[36] Following the resignation of President Nixon in 1974, Congress enacted numerous and enduring reforms, including the Privacy Act of 1974 and major amendments to the Freedom of Information Act.

[27] Most notably for our purposes, Congress passed FISA in 1978. In doing so, Congress in large measure accepted the invitation in *Keith* to create a new judicial mechanism for overseeing national security surveillance. *Under FISA and the Supreme Court's case law, judges retain their power to oversee all electronic surveillance conducted within the United States.* For searches in the criminal context, judges must approve a warrant showing probable cause of a crime. For foreign intelligence searches, the Fourth Amendment continues to apply, because all searches must meet the overall Fourth Amendment test that they be "reasonable."[37] A judge in the Foreign Intelligence Surveillance Court (FISC) can approve a search based on probable cause (the same as for criminal searches), but the standard is that there is probable cause that the search is of "an agent of a foreign power."[38] The original FISA in 1978 and current law are clear – a search of electronic

[36] *See* Swire, *supra* note 1; PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 179 (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter "REVIEW GROUP REPORT"].

[37] *In re Sealed Case*, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002), http://law.justia.com/cases/federal/appellate-courts/F3/310/717/495663/ (describing application of "reasonableness" standard to foreign intelligence searches).

[38] *See* 50 U.S.C. § 1805(a). For additional discussion of the background for how either the criminal or foreign intelligence rules apply, *see* Laura Donohue, *The Fourth Amendment in a Digital World*, 83 U. CHI. L. REV. at note 6 & note 728 (forthcoming 2016), http://ssrn.com/abstract=2726148.

communications within the US is primarily[39] either a criminal investigation (probable cause of a crime) or foreign intelligence investigation (probable cause of an agent of a foreign power).[40]

B. Surveillance after the Attacks of September 11, 2001

[28] Soon after the attacks of September 11, 2001, the US Congress passed the USA PATRIOT Act, which expanded US government surveillance powers in a number of ways. In my view, there were reasons to update surveillance law, but the USA PATRIOT Act swept too broadly.

[29] The Review Group report, of which I was a co-author, explains reasons why foreign intelligence surveillance has faced different challenges after 2001 compared to the intelligence operations of the Cold War.[41] To summarize, during the Cold War the communication systems of the Soviet Union and its allies were largely separate from the communication systems used by the US and Western Europe. During the Cold War, most intelligence operations could happen in "their" country, and not touch the communications of ordinary EU and US citizens. Today, by contrast, there is what the Review Group called the "convergence of civilian communications and intelligence collection." The same communications devices, software, and networks used by EU and US citizens are also used by the targets of intelligence efforts, including terrorist groups and military adversaries. The most deadly targets of surveillance thus often use the communications techniques also used by law-abiding citizens. In my view, it is necessary and appropriate in a democratic society to recognize these changing facts, while crafting effective safeguards against excessive and abusive surveillance.

[30] My 2004 article on "The System of Foreign Intelligence Surveillance Law" discussed many of these changing facts, and provided a detailed description of the legal changes under the USA PATRIOT Act.[42] The article criticized a number of the legal changes, and argued for greater

---

[39] When these searches occur under a mandatory order, they follow either the foreign intelligence or law enforcement regime. 50 U.S.C. § 1802(a) permits a limited collection for a period of a year or less, at the direction of the President and with the approval of the Attorney General, for (1) the collection of communications exclusively between or among foreign powers; and (2) the collection of technical intelligence, which does not include spoken communications of individuals, from property under the control of a foreign power. The government can also gain access to electronic communications with consent.

[40] The importance on the territorial limit on a US judge's jurisdiction and power to issue a search warrant was reinforced this year in *United States v. Microsoft*, where the appellate court held that the presumption against extraterritorial application of law meant that a US judge did not have the power to issue a search warrant on records held outside of the US, in Ireland. 829 F.3d. 197 (2d Cir. 2016), http://www.ca2.uscourts.gov/decisions/isysquery/de5a71a3-b95a-4e0f-a771-f8f9cd131e75/1/doc/14-2985_complete_opn.pdf#xml=http://www.ca2.uscourts.gov/decisions/isysquery/de5a71a3-b95a-4e0f-a771-f8f9cd131e75/1/hilite/. Electronic surveillance conducted outside of the US is done under different legal authorities, often including Executive Order 12,333, discussed below.

Some government access to information does not rise to the level of a "search" under the Fourth Amendment. For instance, under what is called the "third party doctrine," government access to telephone metadata held by a "third party" (the phone company) is permitted constitutionally without a judge-approved warrant. *Smith v. Maryland*, 442 U.S. 735 (1979). In response, Congress in the Electronic Communications Privacy Act of 1986 (ECPA) created statutory protections for telephone metadata, requiring a judicial order by statute rather than it being required by the Constitution. The ECPA is discussed in Chapter 7.

[41] REVIEW GROUP REPORT, *supra* note 36, at 180-87.

[42] Swire, *supra* note 1.

privacy protections. I called for more effective systemic checks against excessive foreign intelligence surveillance.

[31] In preparing this testimony, I carefully re-read the 2004 article, and was encouraged to see roughly ten proposals in the article that now have become the law and practice in the US. For instance, bulk collection of telephone metadata under Section 215 of the USA PATRIOT Act was halted by the USA FREEDOM Act of 2015. The FISC and the Foreign Intelligence Surveillance Court of Review (FISCR), which reviews appeals from the FISC, now benefit from independent briefing by privacy experts. In addition, there are multiple reforms in the transparency and oversight mechanisms. Chapter 2 lists the proposals made in the 2004 article that now have come to fruition.

[32] In light of these and other developments, I am impressed by the quantity and quality of reform of systemic safeguards in the US for foreign intelligence. Chapter 6 discusses the views of the team led by Oxford Professor Ian Brown, who compared current US and other foreign intelligence safeguards. That team concluded that "the US now serves as a baseline for foreign intelligence standards," and the legal framework for foreign intelligence collection in the US "contains much clearer rules on the authorisation and limits on the collection, use, sharing and oversight of data relating to foreign nationals than the equivalent laws of almost all EU Member States."[43] As discussed in the Testimony, these conclusions are essentially equivalent to my own.

C. The Reforms after the Snowden Disclosures

[33] The disclosures by Edward Snowden began in June, 2013. In August 2013, I was named by President Obama as one of five members of the Review Group on Intelligence and Communications Technology. We presented our report of over 300 pages to the President in December. In January 2014, the President made a major speech on surveillance reform. We were told at the time that 70 percent of our 46 recommendations had been adopted in letter or spirit. Others have been adopted since that time. In my view, these reforms demonstrate a democratic response of the US government to concerns raised about surveillance and show a legal system responding to changes in technology.[44]

[34] My testimony in December 2015 to the Belgium Privacy Agency discussed 24 distinct surveillance reforms that the United States undertook from 2013 through the time of the testimony.[45] Since that time, there have been important additional reforms, notably the Privacy

[43] Ian Brown et al., *Towards Multilateral Standards for Surveillance Reform*, 3 (2015), https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf.

[44] In 2013, Jennifer Granick, Director of Civil Liberties for the Center for Internet and Society at Stanford Law School, wrote that the implementation of Recommendation 13 of the Review Group Report would address numerous concerns about how non-US persons are treated under Section 702. Jennifer Granick, *Foreigners and the Review Group Report: Part 2*, JUSTSECURITY.COM (Dec. 19, 2013), https://www.justsecurity.org/4838/foreigners-review-group-report-part-2/. As I have discussed throughout my Testimony, the US has adopted numerous reforms since 2013, including those that respond to Recommendation 13. Specifically, Presidential Policy Directive 28 focuses on these issues and is discussed in Section VI(B) of this Chapter.

[45] As noted in Chapter 2, I presented this testimony as a private citizen, without payment. My testimony in this proceeding expands on the 43 single-spaced pages of the December testimony.

Shield, the Judicial Redress Act, and the Umbrella Agreement on law enforcement sharing. The December testimony discussed these reforms:

A. Independent reviews of surveillance activities

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

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. 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 of FISA;
23. Other changes under Section 702; and
24. Reduced secrecy about National Security Letters.

[35] The discussion in this Chapter now turns to statutory safeguards in the area of foreign intelligence surveillance, followed by an overview of oversight and transparency mechanisms, as well as additional safeguards provided in the executive branch.

III. Statutory Safeguards for Foreign Intelligence Surveillance

[36] This section examines the major statutory safeguards for foreign intelligence surveillance. I will first explain the structure of the FISC and the operation of what are sometimes called "traditional" FISA orders – individual judicial orders authorizing government access to communications of an agent of a foreign power. In connection with discussion of the FISC, the text here summarizes the case study of FISC practices in Chapter 5.

[37] This section then turns to the two major statutory innovations for information collection since 2001. It explains the rules governing Section 215 of the USA PATRIOT Act of 2001, which authorized the collection of bulk telephone metadata. Bulk collection under Section 215 and other statutes was banned by the USA FREEDOM Act of 2015. It then explains the rules governing Section 702 of the FISA Amendments Act of 2008, including discussion of the two programs under Section 702, called PRISM and Upstream. The discussion of Section 702 highlights the original press reports of inaccurate information. We now have authoritative and detailed reports on the actual operations of PRISM and Upstream. Neither authorizes "mass and unrestrained surveillance," and both are under active supervision by federal judges and numerous oversight mechanisms.

A. The Foreign Intelligence Surveillance Court and Traditional FISA Orders

[38] I explain the statutory structure of what is sometimes called "traditional" FISA orders, where there is an individual judicial order to carry out foreign intelligence surveillance. This Section also summarizes my findings based on the review of the FISA-related materials that have been declassified since 2013. Those findings are provided in greater detail in Chapter 5.

1. The Structure of the FISC under FISA

[39] Since passage of FISA in 1978, the FISC has played a central role in regulating the collection of foreign intelligence information by US agencies. In my opinion, the structure of the FISC is an elegant method of governing secret surveillance in an open, democratic society. Independent and high-quality judges gain access to top-secret information, and enforce legal limits on intelligence activities.

[40] The FISC is part of the judicial branch (created by Article III of the Constitution), and independent of the executive branch and the intelligence agencies. FISC judges are selected from among federal district court (trial court) judges. They are nominated to be federal judges by the President, with Senate confirmation. The head of the judicial branch – the Chief Justice of the US Supreme Court – selects the individuals who serve on the FISC for one term of seven years. The Constitution provides structural guarantees to ensure federal judges' independence: federal judges have life tenure, with removal only by impeachment through Congress, and their salary cannot be lowered.[46]

[46] U.S. CONST. art. III. Federal judges are nominated by the President and confirmed by the Senate. *Id.* art II, § 2.

[41] Members of the FISC act in their role as Article III judges, with the same powers that they exercise in their non-FISC cases.[47] FISC judges have full access to classified information. The FISC employs full-time staff attorneys, each of whom is security-cleared and has expertise in national security law. The FISC's Washington, DC chambers are secured so that classified information may be integrated into FISC proceedings.

[42] As shown by its title, the Foreign Intelligence Surveillance Court focuses on foreign intelligence. The statute authorizes wiretaps and other electronic surveillance against "foreign powers."[48] When enacted in 1978, these "foreign powers" included the Communist states arrayed against the US in the Cold War. The definition was broader, however, including any "foreign government or any component thereof, whether or not recognized by the United States."[49] A "foreign power" included a "faction of a foreign nation" or a "foreign-based political organization, not substantially composed of United States persons."[50] Even in 1978, the definition also included "a group engaged in international terrorism or activities in preparation therefor."[51]

[43] FISA judges have jurisdiction to issue orders carried out within the US, upon finding a number of factors, notably that "there is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power."[52] This probable cause standard, with its focus on agents of a foreign power, is different from the wiretap standard, which requires "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense" for which wiretaps are permitted.[53]

[44] FISA orders contain a number of safeguards that also apply to wiretaps in criminal cases. Both regimes require high-level approval within the Department of Justice (DOJ), with the US Attorney General having to give personal approval for FISA applications.[54] Both regimes require minimization procedures to reduce the effects on persons other than the targets of surveillance, as well as to protect content unrelated to the purpose or beyond the scope of the order.[55] Both provide for electronic surveillance for a limited time, with the opportunity to extend the surveillance.[56] Both require details concerning the targets of the surveillance and the nature and location of the

[47] Within the US, the judiciary is a separate branch of government, established by Article III of the US Constitution. *Id.* art. III. US law uses the term "Article III court" to describe federal courts entitled to exercise the full range of judicial power conferred under the US Constitution.
[48] The current definition is codified at 50 U.S.C. § 1801(a).
[49] 50 U.S.C. § 1801(a)(1).
[50] *Id.* §§ 1801(a)(2), 1801(a)(5).
[51] *Id.* § 1801(a)(4).
[52] *Id.* § 1805(a)(3)(A).
[53] 18 U.S.C. § 2518(3)(a).
[54] *Compare* 50 U.S.C. § 1805(a)(2) (approval by the Attorney General for FISA applications), *with* 18 U.S.C. § 2518(11)(b)(i) (approval also permitted for domestic surveillance by the Deputy Attorney General, the Associate Attorney General, or an acting or confirmed Assistant Attorney General). The officers other than the Attorney General who can approve domestic surveillance were added in 1984. Pub. L. No. 98-473, 98 Stat. 2152 § 1203(a) (1984), https://www.gpo.gov/fdsys/pkg/STATUTE-98/pdf/STATUTE-98-Pg1837.pdf .
[55] *Compare* 50 U.S.C. § 1805(a)(4) (FISA applications), *with* 18 U.S.C. § 2518(5) (Title III applications).
[56] *Compare* 50 U.S.C. § 1805(e) (FISA applications), *with* 18 U.S.C. § 2518(5) (Title III applications).

facilities placed under surveillance.[57] Both allow "emergency" orders, where the surveillance can begin without judicial approval subject to quick, subsequent approval by a judge.[58]

[45] As I wrote in the 2004 article, a major difference between the criminal and foreign intelligence orders is that the wiretaps in criminal cases are disclosed to the subject of the surveillance after the fact, but foreign intelligence orders generally are not.[59] My article explained the logic of this difference, which I believe has a strong rationale:

> The secrecy and ex parte nature of FISA applications are a natural outgrowth of the statute's purpose, to conduct effective intelligence operations against agents of foreign powers. In the shadowy world of espionage and counter-espionage, nations that are friends in some respects may be acting contrary to US interests in other respects. Prudent foreign policy may suggest keeping tabs on foreign agents who are in the United States, but detailed disclosure of the nature of that surveillance could create embarrassing incidents or jeopardize international alliances.[60]

[46] Appeals from the FISC go to the Foreign Intelligence Surveillance Court of Review (FISCR). The FISCR, like the FISC, is an Article III court entitled to exercise full constitutional judicial authority, including judicial review. FISCR judges are selected by the Chief Justice of the US Supreme Court from among active federal district or appellate court judges, and serve seven-year terms. The FISCR is exclusively devoted to hearing appeals from FISC rulings. Appeals to the FISCR lie in a number of cases, such as when the FISC denies a government surveillance application,[61] when a communications provider has challenged the legality of government surveillance orders,[62] or when a matter raises uniformity issues for federal case law.[63] Under the USA FREEDOM Act, companies that receive orders from the FISC can challenge these orders and appeal to the FISCR, and even all the way up to US Supreme Court.[64]

[47] As discussed in greater detail in Chapter 5, parties other than the US government have participated more actively over time in the FISC and the FISCR. The USA FREEDOM Act in 2015 created a clear statutory basis for such actions, instructing the FISC to appoint an "*amicus curiae*" (friend of the Court) when the matter at hand presents a novel or significant interpretation

---

[57] *Compare* 50 U.S.C. § 1805(c)(1) (FISA applications), *with* 18 U.S.C. § 2518(4) (Title III applications).

[58] FISA requires an emergency order to receive judicial approval within 7 days. 50 U.S.C. § 1805(e). Title III emergency orders must be approved by a judge within forty-eight hours. 18 U.S.C. § 2518(7).

[59] The individual gains notice of the surveillance when evidence from FISA surveillance is used against an individual in a trial or other proceeding, under the procedures in 50 U.S.C. § 1806. Chapter 8 discusses the similar mechanisms under the Classified Information Protection Act, which seek to provide a fair trial while using classified information.

[60] Swire, *supra* note 1, at 1323.

[61] 50 U.S.C. § 1803(a)(1).

[62] *Id.* §§ 1861(f)(3), 1881a(h)(4)-(5).

[63] *Id.* § 1803(j).

[64] "A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under section 1803(b) of this title, which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision." *Id.*, §§ 1861(f)(3), 1881a(h)(4)-(5).

of the law. *Amicus curiae* are independent experts who are attorneys, provided with access to classified material to allow them to advocate on behalf of privacy and individual rights.[65]

2. Summary of the Case Study on How the FISC Has Applied the Safeguards

[48] Chapter 5 reports on my review of the substantial amount of FISC materials that have been declassified since 2013. The Chapter has four sections, summarized here:

1. *The newly declassified materials support the conclusion that the FISC today provides independent and effective oversight over US government surveillance*. Especially since the Snowden disclosures, the FISC was criticized in some media outlets as a "rubber stamp." This section shows that this claim is incorrect. It examines FISC opinions illustrating the Court's care in reviewing proposed surveillance. For many years, an important role of the FISC was to insist that the Department of Justice clearly document its surveillance requests, with the effect the Department would only go through that effort for high-priority requests. Since the passage of the USA FREEDOM Act, the number of surveillance applications that the FISC has modified or rejected has, at least initially, grown substantially, to 17 percent of surveillance applications in the second half in 2015. The section closes by showing the FISC's willingness to exercise its constitutional power to restrict surveillance that it believes is unlawful.

2. *The FISC monitors compliance with its orders, and has enforced with significant sanctions in cases of noncompliance*. The FISC's jurisdiction is not confined to approving surveillance applications. The FISC also monitors government compliance and enforces its orders. This section outlines the system of rules, third-party audits, and periodic reporting that provide the FISC with notice of compliance incidents. It then discusses examples of the FISC's responses to government noncompliance. FISC compliance decisions have resulted in (a) the NSA electing to terminate an Internet metadata collection program; (b) substantial privacy-enhancing modifications to the Upstream program; (c) the deletion of all data collected via Upstream prior to October 2011; and (d) a temporary prohibition on the NSA accessing one of its own databases.

3. *In recent years, both the FISC on its own initiative and new legislation have greatly increased transparency.* Under the original structure of FISA, enacted in 1978, the FISC in many respects was a "secret court" – the public knew of its existence but had very limited information about its operations. This section describes how, in recent years, the FISC itself began to release more of its own opinions and procedures, and the USA FREEDOM Act now requires the FISC

[65] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act of 2015), Pub. L. No. 114-23, § 401 (2015), https://www.gpo.gov/fdsys/pkg/PLAW-114publ23/html/PLAW-114publ23.htm.

to disclose important interpretations of law. It also discusses how litigation before the FISC resulted in transparency reporting rights, and how these rights have been codified into US surveillance statutes.

4. *The FISC now receives and will continue to benefit from briefing by parties other than the Department of Justice in important cases.* Originally, the main task of the FISC was to issue an individual wiretap order, such as for one Soviet agent at a time. As with other search warrants, these proceedings were *ex parte*, with the Department of Justice presenting its evidence to the FISC for review. After 2001, the FISC played an expanded role in overseeing entire foreign intelligence programs, such as under Section 215 and Section 702. In light of the more legally complex issues that these programs can raise, there was an increasing recognition that judges would benefit from briefing by parties other than the Department of Justice. This section reviews newly declassified materials concerning how the FISC began to receive such briefing, of its own initiative. Prior to the USA FREEDOM Act, the FISC created some opportunities for privacy experts and communication services providers and civil society groups to brief the court. The USA FREEDOM Act has created a set of six experts in privacy and civil liberties who will have access to classified information and will brief the court in important cases.

B. Collection of Documents and Other Tangible Things under Section 215

[49] Perhaps the most dramatic change in US surveillance law since 2013 concerns Section 215 of the USA PATRIOT Act, which provided the government with broad powers to obtain "documents and other tangible things."[66] Section 215 was an early target of concern for civil liberties defenders after it was created, and I wrote a detailed critique in 2005 of why the law appeared too favorable to the government.[67] Even given my concerns about overbroad use of Section 215, I personally was surprised in June 2013 when we learned details about the government's telephone metadata program, which used "foreign intelligence" authorities as a basis for collecting metadata on massive numbers of domestic US to domestic US telephone calls.[68]

[50] The concern about over-broad collection made bulk collection under Section 215 a major focus of our work on the Review Group. As part of that work, members of the Review Group individually reviewed over fifty cases where the intelligence community said that intelligence authorities had prevented a terrorist attack since 2001. Based on that individual review, and drawing on the decades of experience of Review Group members within the intelligence community, the Review Group's Report stated: "Our review suggests that the information contributed to terrorist investigations by the use of Section 215 telephony metadata was not

[66] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. 107-56, § 215 (2001) ("Access to records and other items under the foreign intelligence surveillance act"), https://apps.americanbar.org/natsecurity/patriotdebates/act-section-215.

[67] Peter Swire, Reply to *Why Sections 215 and 215 Should be Retained*, PATRIOT DEBATES: A SOURCEBLOG FOR THE USA PATRIOT DEBATE, AMERICANBAR.ORG (2005), http://apps.americanbar.org/natsecurity/patriotdebates/214-and-215-2#rebuttal.

[68] The telephone metadata program was accompanied by a similar Internet metadata program that was the subject of strict oversight by the FISC in 2009-10 and then was terminated by the NSA, as discussed in Chapter 5.

essential to preventing attacks and could readily have been obtained in a timely manner using conventional Section 215 orders."[69] This finding of "not essential to preventing attacks" had credibility because it was based on top-secret briefings to a group that contained senior experts in intelligence and counter-terrorism. A common response to civil liberties concerns says: "If you knew what we knew, you would want this surveillance power." After the Review Group report, that response was much harder to make in defense of Section 215 bulk collection.

[51] Consistent with the Review Group's Report, and similar recommendations from the PCLOB, the Obama Administration by 2014 took a number of measures to limit bulk collection under Section 215. President Obama stated that his Administration would "transition away" from bulk collection of telephony metadata.[70] He ordered the Attorney General to develop a "new approach" where US intelligence agencies would no longer collect and store metadata themselves.[71] During this transition period, President Obama ordered that (1) the NSA could only query the telephony metadata database upon approval by the FISC; and (2) NSA queries could only pursue phone calls two steps removed from the original "seed" number.[72]

[52] The USA FREEDOM Act put these and similar safeguards into statutory form. That Act amended Section 215 so that it can authorize requests for records of individuals, but not bulk collection.[73] The Act went further, putting the same prohibition on bulk collection on the two other authorities that the government could potentially have invoked for similar bulk collection: (1) FISA pen register and trap and trace authorities (to/from information about communications);[74] and (2) National Security Letters (phone, financial, and credit history records).[75] These clear statements in law from Congress plainly state the limits on appropriate use of Section 215 and other authorities. I believe such clear legislation from Congress also put agency lawyers and other employees on notice that they should be cautious in stretching any other authorities to reach similar ends.

[53] In the wake of the USA FREEDOM Act, the program for government storage of bulk telephone metadata storage was shut down.[76] The Act established a new system under Section 215 for access to call records in terrorism investigations. Under the new system, the government must identify a specific selector that is reasonably suspected of being associated with terrorism. In identifying such selectors, the government can only obtain records that are no more than "2 hops" away – information about one telephone number, for instance, can be used to justify a search of those who called the number (one hop), and those who called those callers (two hops), but not any

---

[69] REVIEW GROUP REPORT, *supra* note 36, at 104.
[70] *See* President Barack Obama, Remarks by the President on Review of Signals Intelligence, WHITE HOUSE, OFFICE OF THE PRESS SEC'Y (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
[71] *Id.*
[72] *Id.*
[73] USA FREEDOM Act, Pub. L. No. 114-23, § 103 (2015).
[74] *Id.* § 201.
[75] *Id.* § 501.
[76] The program ended in November 2015. *See, e.g.*, Cody Poplin, *NSA Ends Bulk Collection of Telephony Metadata Under Section 215*, LAWFAREBLOG, (Nov. 30, 2015), https://www.lawfareblog.com/nsa-ends-bulk-collection-telephony-metadata-under-section-215.

further. Instead of the pre-2013 procedure of having requests approved within the NSA, any such individual requests under Section 215 now must receive judicial approval in the FISC.[77]

[54] In conclusion on Section 215, the US has now created strong, statutory safeguards against bulk collection under Section 215, the FISA trap-and-trace authority, and National Security Letters. In my view, the independent investigations by the Review Group and the PCLOB contributed to an informed public debate, leading to notable new limits on foreign intelligence collection. These limits on bulk collections apply to investigations concerning both US and non-US persons.

C. Collection of Electronic Communications under Section 702

[55] This section explains the legal structure of Section 702 of FISA 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.[78]

1. The Legal Structure of Section 702

[56] The rationale for what is commonly referred to as Section 702 evolved from the changing nature of international communications.[79] 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 Ireland and someone in Pakistan could be collected either in Ireland 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 an Irish person in Ireland and a Pakistani person 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. The EU and other democracies have similarly given themselves greater freedom to do surveillance outside of their borders than within.

---

[77] USA FREEDOM Act § 104.

[78] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 2 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf [hereinafter "PCLOB 702 REPORT"].

[79] "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. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 ("FISA Amendments Act of 2008"), Pub. L. 110-261 (2008), https://www.govtrack.us/congress/bills/110/hr6304/text.

[57] With the rise of the Internet, the facts changed. Now, the same communication between Ireland and Pakistan quite possibly did pass through the US – 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[80] when the intercept occurred within the US.[81] 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,[82] Congress passed Section 702 of FISA in 2008.

[58] 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.[83] To target the communications of any person, the government must have a foreign intelligence purpose to conduct the collection and a reasonable belief that the person is a non-US citizen located outside of the US.[84] Section 702 can provide access to the full contents of communications, and not just metadata such as 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 below in connection with Presidential Policy Directive 28 (PPD-28), the Administration has agreed to strengthen the targeting rules.[85] The court annually also approves minimization procedures, to cover the acquisition, retention, use, and dissemination of non-publicly available information about US persons.[86]

---

[80] This type of non-US to non-US communication was historically handled under Exec. Order No. 12,333, 3 C.F.R. 200 (1981 Comp.), *reprinted in* 50 U.S.C. § 401 (Supp. V 1981), http://www.archives.gov/federal-register/codification/executive-order/12333.html.

[81] This type of communication was historically governed by the stricter standards of the Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. 95-511, 92 Stat. 1783 (1978), https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286.

[82] Laura 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"), http://scholarship.law.georgetown.edu/facpub/1355/.

[83] For discussion of the numerous specific requirements in Section 702, *see id.*; *see also* NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE, NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 (Apr. 16, 2014), https://www.nsa.gov/about/civil-liberties/reports/assets/files/nsa_report_on_section_702_program.pdf.

[84] REVIEW GROUP REPORT, *supra* note 36, Appendix A at 263.

[85] 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 samples 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 audits.

[86] ELECTRONIC PRIVACY INFORMATION CENTER, *Foreign Intelligence Surveillance Court (FISC)*, EPIC.ORG, https://epic.org/privacy/surveillance/fisa/fisc/.

[59] 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 what critics have called "unrestricted access to mass data"[87] 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 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 EU 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.[88]

The PCLOB's report on Section 702 provides step-by-step examples about how these and other safeguards apply in practice.[89] As one example, key words and names of targeted individuals cannot be used as selectors.[90]

[60] Section 702 provides more detailed legal restrictions than applied previously to non-US to non-US communications. Previously, if the US conducted surveillance overseas, to target foreign communications, the US Constitution and other laws did not limit US government activities.[91] 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. Put simply, communications of EU persons accessed in the US under Section 702 are governed by the full set of statutory and judicial safeguards, in contrast to the lack of similar statutory protections of EU persons prior to the 2008 amendments.

---

[87] The Advocate General's opinion in the original *Schrems v. Facebook* case stated that the PRISM program provided "unrestricted access to mass data." THE IT LAW COMMUNITY, *Not so Safe Harbour: Advocate General's Opinion in Schrems*, SCL.ORG (Sep. 23, 2015), http://www.scl.org/site.aspx?i=ne44089.

[88] REVIEW GROUP REPORT, *supra* note 36, Appendix B at 267.

[89] PCLOB 702 REPORT, *supra* note 78, at 46.

[90] "[S]electors may not be key words (such as 'bomb' or 'attack'), or the names of targeted individuals ('Osama Bin Laden')." PCLOB 702 REPORT, *supra* note 78, at 33.

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

2. Popular Misunderstandings of the PRISM Program

[61] 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. 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.

[62] 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 judicially-approved and judicially-supervised directive requiring collection of certain "selectors," such as an email address. The directive goes to a US-based service provider. The company's 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.[92]

[63] 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 US Internet companies, extracting audio, video, photographs, emails, documents, and connection logs that enable analysts to track a person's movements and contacts over time."[93] We now know 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.

[64] The inaccuracies in the news story led to immediate responses. Technology companies named in the article[94] issued statements denying that the government had direct access to their servers to collect user data.[95] Within 24 hours, the *Washington Post* itself heavily edited the original story. The lead sentence no longer stated that there was direct access by the NSA, but instead said there was direct access "according to a top-secret document obtained by The Washington Post."[96] The document the story relied on, a PowerPoint presentation about the PRISM program, was incorrect when it stated that the NSA had direct access to the servers.

---

[92] PCLOB 702 REPORT, *supra* note 78, at 7.

[93] Barton Gellman, *U.S. intelligence mining data from nine U.S. Internet companies in broad secret program*, THE WASHINGTON POST (Jun. 6, 2013) (emphasis added). 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. *See* Bryan Preston, *WaPo Quietly Changes Key Details in NSA Story*, PJ MEDIA (Jun. 11, 2013), 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). Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, THE WASH. POST (Jun. 7, 2016), 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.

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

[95] Chenda Ngak, *Apple, Google, Facebook, Yahoo, Microsoft, Paltalk, AOL issue statements of denial in NSA data mining*, CBS NEWS (Jun. 7, 2013), http://www.cbsnews.com/news/apple-google-facebook-yahoo-microsoft-paltalk-aol-issue-statements-of-denial-in-nsa-data-mining/.

[96] Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, THE WASHINGTON POST (Jun. 7, 2016),

[65] 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.[97] The Review Group and PCLOB 702 reports, based on review of classified material, both described the Section 702 program as it is described here, with no direct access to the servers.[98]

[66] 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:*[99]

> 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.[100]

[67] 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 US owned or controlled by a range of companies active in the Internet and technology field, such as Facebook USA."[101] The opinion added that, for information transferred by a company such as Facebook to the US, there is "mass, indiscriminate surveillance."[102]

---

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.

[97] *See* Richard Lawler, *Washington Post: NSA, FBI tapping directly into servers of 9 leading internet companies (update)*, ENGADGET (Jun. 6, 2013), https://www.engadget.com/2013/06/06/washington-post-nsa-fbi-tapping-directly-into-servers-of-9-lea/; Declan McCullagh, *No evidence of NSA's 'direct access' to tech companies*, C|NET (Jun. 7, 2013), http://www.cnet.com/news/no-evidence-of-nsas-direct-access-to-tech-companies/; Henry Blodget, *The Washington Post Has Now Hedged Its Stunning Claim About Google, Facebook, Etc, Giving The Government Direct Access To Their Servers*, BUSINESS INSIDER (Jun. 7, 2013), http://www.businessinsider.com/washington-post-updates-spying-story-2013-6.

[98] *See* PCLOB 702 REPORT, *supra* note 78, at 33-34; REVIEW GROUP REPORT, *supra* note 36, at 134-42.

[99] *Schrems v. Data Prot. Comm'r* [2014] IEHC 310, (H. Ct.), http://www.courts.ie/Judgments.nsf/0/481F4670D038F43380257CFB004BB125.

[100] *Id.*

[101] Case C-362/14, *Opinion of Advocate General Bot* in *Schrems v. Data Prot. Comm'r*, para. 26 (Sept. 23, 2015) (emphasis added), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=168421.

[102] *Id.* para. 200.

[68] These sensational but incorrect factual assertions are a close fit with the crucial statement by the European Court of Justice that the US lacks "a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order."[103]

[69] I wrote about these incorrect factual assertions in my December 2015 testimony to the Belgian Privacy Authority, and no one has sought to challenge any of the facts. The correction has also been understood by leading European and US institutions. The European Union Agency for Fundamental Rights released a major report about surveillance by intelligence services, at the request of the European Parliament.[104] 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*[105] 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."[106] The Agency for Fundamental Rights report quoted the Cayford article statement that PRISM is "'a targeted technology used to access court ordered foreign Internet accounts," and not mass surveillance.[107] 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-US] persons about whom an individualized determination has been made."[108]

[70] 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,[109] with the statistics subject to oversight from Congress, Inspectors General,

---

[103] Case C-362/14, *Schrems v. Data Prot. Comm'r*, para. 96 (E.C.J.) (Oct. 6, 2015), http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=2393.

[104] European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2015), http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf [hereinafter *European Union Agency for Fundamental Rights Report*].

[105] *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. Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google, and others*, THE GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. The slide speaks of PRISM "collection directly from the servers" of nine US Internet service providers. *Id.*

[106] M. Cayford, et al., *All Swept Up: An Initial Classification of NSA Surveillance Technology*, in SAFETY AND RELIABILITY: METHODOLOGY AND APPLICATIONS, 645-46 (Nowakowski, et al. eds. 2015), http://www.crcnetbase.com/doi/pdfplus/10.1201/b17399-90. The *European Union Agency for Fundamental Rights Report*, which reviewed the PRISM program in light of the Cayford article, 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 Report*, *supra* note 104, at 17.

[107] *European Union Agency for Fundamental Rights Report*, *supra* note 104, at 17.

[108] PCLOB 702 REPORT, *supra* note 78, at 111.

[109] The first three have been released: OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2015* IC ON THE RECORD (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015; OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2014*, IC ON THE RECORD (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014; OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual*

the FISC, the PCLOB, and others.[110] In 2015, there were 94,368 "targets" under the Section 702 programs, many of whom are targeted due to evidence linking them to terrorism.[111] 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.[112]

3. The Upstream Program

[71] In addition to PRISM, Section 702 supports intelligence collection commonly referred to as the "Upstream" program. The PCLOB reported, "Upstream collection is different from PRISM collection because the acquisition occurs not with the compelled assistance of United States [Internet service providers], but instead with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications backbone over which communications transit."[113] Like PRISM, Upstream was developed as a response to changing technology. As the Internet developed, a large portion of the Internet backbone passed through the US, meaning that many foreign-to-foreign communications could be accessed by surveillance done inside the US. Upstream targets Internet-based communications as they pass through physical Internet infrastructure located within the US.

[72] As I testified before the Belgian Privacy Authority, Upstream is better viewed as a targeted program, and not as "mass surveillance."[114] Upstream is designed to only acquire Internet communications that contain a tasked selector. To do so, Upstream filters Internet transactions that pass through the Internet backbone to eliminate potential domestic transactions; these are then further screened to capture only transactions containing a tasked selector.[115] Emails and other transactions that make it through the filters are stored for access by the NSA, while information that does not make it through the filters is never accessed by the NSA or anyone else.[116]

Statistics for Calendar Year 2013, IC ON THE RECORD (June 26, 2014), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.

[110] For a listing of the multiple oversight entities, *see* REVIEW GROUP REPORT, *supra* note 36, at Appendix C.

[111] 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. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2015*, IC ON THE RECORD (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015

[112] 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." OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2014*, IC ON THE RECORD (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

[113] PCLOB 702 REPORT, *supra* note 78, at 35.

[114] Swire, *US Surveillance Law*, *supra* note 25, at 17-18.

[115] *See* PCLOB 702 REPORT, *supra* note 78, at 37 ("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.").

[116] As I testified before the Belgian Privacy Authority, I believe "the NSA has built a large and generally effective compliance program in recent years" to enforce these restrictions, and that "[s]ystematic violation of the Section 702 rules would thus be highly risky for the NSA to undertake." *See* Swire, *US Surveillance Law*, *supra* note 25, at 18 n.65.

Importantly, Upstream uses selectors such as telephone numbers or email addresses – they cannot be key words or names of individuals.[117]

[73] In addition to technical safeguards, Upstream collection is comparatively small in relation to other NSA programs.[118] Communications collected via Upstream are subject to separate and more restrictive minimization measures than other surveillance programs.[119] For these reasons, the PCLOB's 2014 review found that Section 702 programs are "not based on the indiscriminate collection of information in bulk."[120] Instead, "the government acquires only those communications involving [] particular selector[s]."[121]

D. Conclusion on Section 702

[74] Concerning both Upstream and PRISM, and based on classified briefings, the PCLOB found:

> Unlike the telephone records program conducted by the NSA under Section 215 of the USA PATRIOT Act [which has since been repealed], 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-US 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.[122]

[75] In conclusion on Section 702, the public record is much more complete than it was at the time of the initial Snowden disclosures in June 2013. The original PRISM press report incorrectly stated that the NSA had direct access into the service providers' databases. Early discussions of the Upstream program imagined that the number of individuals whose information was accessed was immense. Based on authoritative reports by independent judges in the FISC and independent reviews by the Review Group and the PCLOB, the facts are much different. The number of individuals targeted by the program is far lower than many supposed. As discussed in Chapter 5,

---

[117] PCLOB 702 REPORT, *supra* note 78, at 36-39. The PCLOB provides the following example of how this restriction would work in day-to-day Upstream collection: "If the NSA . . . task[ed] email address 'JohnTarget@example.com,' to Section 702 upstream collection, the NSA would potentially acquire communications routed through the Internet backbone that were sent from email address JohnTarget@example.com, that were sent to JohnTarget@example.com, and communications that mentioned JohnTarget@example.com in the body of the message. The NSA would not, however, acquire communications simply because they contained the name 'John Target.'" *Id.* at 37.

[118] A declassified FISC opinion found that over 91% of the Internet communications obtained by the NSA in 2011 under Section 702 actually resulted from PRISM, with approximately 9% coming from Upstream. *See [Caption Redacted]*, No. [Redacted], 2011 WL 10945618 (F.I.S.C. Oct. 3, 2011), at 30, 33-34, https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

[119] PCLOB 702 REPORT, *supra* note 78, at 50-66.

[120] *Id.* at 111.

[121] *Id.*

[122] *Id.*

Section 702 was already under vigorous judicial oversight. In addition, as discussed further below in this Chapter in connection with the PCLOB, numerous independent agency recommendations have been implemented since 2013.

[76] Section 702 sunsets at the end of 2017, so Congress will address reform issues in 2017 because the authority expires unless Congress passes new authorization and the President signs it. There will be a public debate on possible amendments, as there was in connection with the Section 215 sunset in 2015. The EU and its data protection experts have an opportunity to recommend amendments, and we saw with the Judicial Redress Act that EU concerns can have an impact on US legislative deliberations. Even in the absence of such reforms, however, Section 702 has a far more comprehensive set of safeguards than was apparent in 2013.

IV. Oversight Mechanisms

[77] There is a comprehensive oversight system for foreign intelligence, including Senate and House intelligence committees, agency Inspectors General, the independent Privacy and Civil Liberties Oversight Board, and Privacy and Civil Liberties offices in the agencies. Each of these institutions gains access to the classified information needed to provide oversight. In addition to the safeguards provided by FISA, structural safeguards exists in the legislative and executive branches, as well as by an ongoing independent oversight board.[123] After the Snowden revelations, the Review Group that I served on was convened to conduct a one-time review.

A. Executive Agency Inspectors General

[78] The federal inspector general (IG) component provides a well-staffed and significant safeguard to ensure that federal agencies comply with internal administrative privacy mandates, and that federal agencies comply with and enforce federal laws mandating privacy guarantees for US and non-US persons. The federal IGs were created by the Inspector General Act of 1978 in order to establish IG offices within departments and agencies of the federal government.[124] The IG creates an independent and objective unit within these agencies and departments in order to:

1. "conduct and supervise audits and investigations relating to the programs and operations" of the departments or agencies within which they function;

2. "provide leadership and coordination and recommend policies for activities designed to (A) to promote economy, efficiency, and effectiveness in the

[123] *See generally* U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE, SENATE.GOV, http://www.intelligence.senate.gov/; U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE, HOUSE.GOV, http://intelligence.house.gov/; IC INSPECTOR GENERAL, DNI.GOV, https://www.dni.gov/index.php/about/leadership/inspector-general#; PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, PCLOB.GOV, https://pclob.gov/. Recent PCLOB reports include: PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf and PCLOB 702 REPORT, *supra* note 78.

[124] Inspector General Act of 1978, 5 U.S.C. App. 3 §§ 2, 12.

administration of, and (B) to prevent and detect fraud and abuse in such programs and operations"; and

3. "to provide a means for keeping the head of the establishment and the Congress fully and currently informed about the problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action."[125]

Thus, the IG supplements and publicly reports deficiencies in internal compliance generally, and reports specific deficiencies or violations. The IG also acts as a Whistleblower Protection Ombudsman for the purposes of educating employees about the "prohibitions on retaliation for protected disclosures;" and for advising potential whistleblower employees about the "rights and remedies against retaliation for protected disclosures."[126]

[79] The Inspector General's privacy watchdog responsibilities include instances where employees violate the privacy of government employees as well as ordinary citizens. For example, in 2015 Department of Homeland Security IG John Roth issued a report detailing misconduct by agents of the US Secret Service for improper access to sensitive information in violation of the Privacy Act, as well as internal agency employment rules incorporating additional mandates for privacy protection and the handling of sensitive information.[127] The report detailed the misconduct to the head of the agency, found the allegations to be valid, authorized employee sanctions, and identified potential violations of the law for further investigation.[128] In August 2016, the IG office within US Customs and Border Protection (CBP) found that the CBP improperly shared sensitive personal information with 30 agencies in violation of the Privacy Act.[129] The report concluded, "we believe the manner in which [Customs investigators] shared the sensitive [information] showed a lack of regard for, and may have compromised, these individuals' privacy."[130] The IG stated it "attribute[d] this to [the agency's] general belief that accomplishing its law enforcement mission takes precedence over its responsibility to protect [an] individual's privacy."[131] The IG concluded that privacy takes priority, demonstrating the critical check and balance the IG role plays in the US government's implementation and enforcement of privacy-related issues.[132]

[80] Individuals serving within any organization with an IG are able to report waste, fraud, and abuse in a way that the sensitive material remains confidential, while problems are brought to the attention of the appropriate authorities. The IGs meet with the Intelligence Community Inspector

---

[125] *Id.* § 2.
[126] *Id.* § 3.
[127] JOHN ROTH, DEPARTMENT OF HOMELAND SECURITY OFFICE OF INSPECTOR GENERAL, INVESTIGATION INTO THE IMPROPER ACCESS AND DISTRIBUTION OF INFORMATION CONTAINED WITHIN A SECRET SERVICE DATA SYSTEM, 14-17 (Sep. 25, 2015), https://www.oig.dhs.gov/assets/Mga/OIG_mga-092515.pdf.
[128] *Id.* at 3-14.
[129] DEPARTMENT HOMELAND SECURITY, OFFICE OF INSPECTOR GENERAL, CBP'S OFFICE OF PROFESSIONAL RESPONSIBILITY'S PRIVACY POLICIES AND PRACTICES, OIG-16-123 (Aug. 29, 2016), https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-123-Aug16.pdf.
[130] *Id.* at *2 (Section titled "What We Found").
[131] *Id.*
[132] *Id.*

General on a regular basis to address concerns that span more than one organization.[133] Every agency in the intelligence community, including the NSA, has an IG.

B. Legislative Oversight

[81] The US has a lengthy history of oversight of foreign intelligence. In the wake of the Watergate scandal and Church Commission findings in the late 1970s, Congress created the Senate and House Intelligence Committees, which receive classified briefings about intelligence surveillance. The 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.[134] In addition, the Congressional Research Service makes publicly available reports on surveillance topics.[135]

[82] Based on my experience and discussions with others, individual members and their staff on these committees regularly ask probing questions in closed session or privately about areas or incidents of concern. The intelligence committees also have in some instances been harshly critical of intelligence agencies in public. A notable recent example is a large and critical study of the Central Intelligence Agency's activities related to torture, published in 2014.[136]

[83] In 1976, the US Senate created the US Senate Select Committee on Intelligence to oversee the intelligence activities of the US government, to submit proposals for legislation to the Senate, and to provide vigilant legislative oversight. The Committee is composed of 15 Senators who have access to intelligence sources and methods, programs, and budgets. Through the use of staff members (who along with the Senators have access to classified material), the Committee engages in daily oversight of intelligence activities. The Committee regularly conducts closed hearings to hear from senior intelligence officials. At least once a year, the Committee holds a public hearing to receive testimony on national security threats.[137]

---

[133] IC INSPECTOR GENERAL, *Who We Are*, DNI.GOV, https://www.dni.gov/index.php/about/organization/office-of-the-intelligence-community-inspector-general-who-we-are.

[134] *See generally* C-SPAN, *Cybersecurity Threats, Admiral Michael Rogers, National Security Agency (NSA) Director & U.S. Cyber Command Commander* (remarks at the National Press Club, Washington, DC on Jul. 16, 2016 regarding cybersecurity challenges and his role protecting the US from cyber threats), https://www.c-span.org/video/?412319-1/nsa-director-michael-rogers-discusses-cybersecurity-threats.

[135] FEDERATION OF AMERICAN SCIENTISTS, *Congressional Research Service Reports on Intelligence and Related Topics*, http://www.fas.org/sgp/crs/intel/index.html.

[136] SENATE SELECT COMMITTEE ON INTELLIGENCE, COMMITTEE STUDY OF THE CENTRAL INTELLIGENCE AGENCY'S DETENTION AND INTERROGATION PROGRAM (2014), http://www.intelligence.senate.gov/press/committee-releases-study-cias-detention-and-interrogation-program.

[137] U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE, *Overview of the Senate Select Committee on Intelligence Responsibilities and Activities*, SENATE.GOV, http://www.intelligence.senate.gov/about.

[84] The US House of Representatives Permanent Select Committee on Intelligence was created in 1977, with a similar function to the US Senate Select Committee on Intelligence.[138] The Permanent Select Committee is comprised of 22 members of Congress.

[85] Along with their other oversight roles, these intelligence committees can receive direct reports from whistleblowers regarding classified information. Under the Intelligence Community Whistleblower Protection Act of 1998, employees and contractors of specific federal intelligence agencies may report serious problems related to intelligence activities directly to the Senate and House intelligence committees.[139] These complaints, when they concern classified information, are permitted for a "serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity."[140] As one example of a relevant Presidential order, PPD-28 requires agencies to "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."[141] The broad protections under PPD-28, including minimization and dissemination protections, are discussed below in the discussion of executive branch safeguards. A serious problem in following the dictates of PPD-28 would thus appear to qualify for an employee to go directly to the congressional committees, even for classified information.

[86] Under this whistleblower law, an employee or contractor must report the concern first to the appropriate Office of the Inspector General (OIG). That OIG then has 14 days to determine "whether the complaint or information appears credible."[142] If the OIG determines the petition is credible, that information is then transferred to the House and Senate Intelligence Committees for their review.[143] If the OIG does not believe the complaint or information is credible, the petitioner may directly provide the same information to the House and Senate Committees after informing the OIG of his or her intention to do so.[144] The petitioner must still follow the procedures of the Act in doing so in order to protect the relevant classified information. Thus, violations of a law, PPD-28, or other Presidential orders that protect non-US persons can form the basis for a whistleblower report to Congress, even for classified information.

C. Independent Review: Review Group and PCLOB

[87] Since the Snowden revelations, practices of the NSA and the rest of the intelligence community have been reviewed by two independent entities – the ongoing Privacy and Civil

---

[138] U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE, *History and Jurisdiction*, HOUSE.GOV, http://intelligence.house.gov/about/history-and-jurisdiction.htm. The US House of Representatives maintained a Select Committee on Intelligence from 1975 to 1977.
[139] 5 U.S.C. § 8H(d)(2).
[140] *Id.* § 8H(i)(1).
[141] THE WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, Presidential Policy Directive, Signals Intelligence Activities, PPD-28 (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter "PPD-28"].
[142] 5 U.S.C. App. 1 § 8H(a)(1).
[143] *Id.* § 8H(b).
[144] *Id.* § 8H(d).

Liberties Oversight Board[145] and the Review Group on which I served.[146] I discuss the Review Group elsewhere, including in Chapter 2.

[88] The PCLOB has essentially the same independent agency structure as the Federal Trade Commission (FTC). 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 the highest level security clearances – Top Secret/Special Compartmented Information (TS/SCI) – and investigate and report on the counterterrorism activities of the US intelligence community.[147] The statute creating the Board provides that it "shall continually review" agencies engaged in anti-terrorism activities "to determine whether such actions appropriately protect privacy and civil liberties and are consistent with governing laws, regulations, and policies regarding privacy and civil liberties."[148] The PCLOB has substantial powers to investigate intelligence community practices, including the ability (1) to "have access from any department … to all relevant records";[149] (2) to interview personnel from any department;[150] and (3) to request the Attorney General to issue a subpoena for records held by individuals for any relevant information.[151]

[89] The PCLOB is an independent privacy agency with substantial investigative powers over foreign intelligence activities. In protecting individuals, the PCLOB has the notable advantage of having access to the classified information that it believes it needs to do its job.

[90] Since 2013, the PCLOB has released detailed reports on Section 215 and 702 programs, making numerous recommendations.[152] Its central recommendations on the telephone metadata program were enacted in the USA FREEDOM Act. It made ten recommendations concerning Section 702, and virtually all have been accepted and either implemented or are in the process of being implemented. To my direct knowledge, the 46 recommendations from the Review Group became a checklist for the Obama Administration, so that each recommendation was either adopted or there was extensive deliberation about why it should not be adopted.[153] I believe a

[145] The PCLOB, at the time of these reports, had 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 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. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *Board Members*, PCLOB.gov, https://pclob.gov/about-us/board.html.

[146] The recommendations of the Review Group, as well as discussion of the implementation that has occurred since the release of our report, are detailed in Chapter 6.

[147] OFFICE OF JUSTICE PROGRAMS, THE IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007, Pub. L. 110-53 (Aug. 3, 2007), https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1283.

[148] 42 U.S.C. § 2000ee(d)(2).

[149] *Id.* § 2000ee(g)(1).

[150] *Id.*

[151] *Id.* § 2000ee(g)(2).

[152] *See, e.g.*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

[153] As mentioned above at Sec. II (C) "The Reforms after the Snowden Disclosures," members of the Review Group were told in early 2014 that 70 percent of the 46 recommendations had been adopted in letter or in spirit.

similar procedure was followed for the PCLOB recommendations. Taken together, my view is that this shows considerable impact of independent review on post-Snowden surveillance practices.

[91] To illustrate the impact of the PCLOB's independent review, I examine the ten recommendations about Section 702 that it issued in its 2014 report:

1. *The NSA's targeting procedure should require written explanation of the basis for targeting to allow a determination that the targeting of each selector is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISC.* As part of the annual certification process for the Section 702 program, the NSA revised targeting procedures for approval by the FISC.[154]

2. *The FBI's minimization procedures should be clarified to more clearly reflect the practices for conducting US person queries. Particularly, even though FBI analysts who work on non-foreign intelligence crimes are not required to conduct queries of databases containing Section 702 data, they are permitted to conduct such queries.* As part of the annual certification process for the Section 702 program before the FISC, the FBI revised its minimization procedures to better reflect its procedures.[155]

3. *The NSA and CIA minimization procedures should permit these agencies to query collected Section 702 data for foreign intelligence purposes using US persons identifiers only if the query is based on a statement showing that it is reasonably likely to return foreign intelligence information.* As part of the annual certification process for Section 702, the NSA and CIA submitted revised minimization procedures that addressed this recommendation.[156]

4. *As part of the FISC's consideration of Section 702 certification applications, the government should provide a random sample of targeting decisions that would allow the FISC to take a retrospective look at the targets selected over the course of a recent time period.* The FISC reported that the government provided the Court's legal staff with a brief on its oversight activities as well as sample tasking sheets and query terms.[157]

---

[154] The PCLOB recommended that NSA targeting procedures specify criteria for determining the expected foreign intelligence value for a particular target. *See* PCLOB 702 REPORT, *supra* note 78, at 11, 134-37. The PCLOB considers that this portion of the recommendation is only partially implemented, as the targeting procedure provide somewhat more detail in procedure, but do not clarify substantive criteria. *Id.*

[155] *Id.* at 11-12, 137-39. The PCLOB found that clarifying the FBI's practice in written minimization procedures is "important for accountability and transparency," and would "better enable the [FISC] to assess statutory and constitutional compliance" going forward. *Id.* at 137.

[156] *Id.* at 12, 139-40. For example, the CIA's minimization procedures now provide that "[a]ny United States person identity used to query the content of communications must be accompanied by a statement of facts showing that [it] is reasonably likely to return foreign intelligence information." OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CIA 2015 MINIMIZATION PROCEDURES, 3 (July 15, 2015), https://www.dni.gov/files/documents/2015CIAMinimizationProcedures_Redacted.pdf.

[157] *Id.* at 12, 141.

5. *As part of the periodic certification process, the government should incorporate into its submission to the FISC the rules for operation of the Section 702 program that have not already been included in certification orders before the FISC.* During the certification process, the government submitted a summary of notable Section 702 requirements.[158]

6. *To enhance current efforts to filter upstream communication, the NSA and DOJ should work with telecommunications companies to periodically assess filtering techniques to ensure government acquisition of only communications that are authorized for collection.* The NSA conducted a review, and reported to the PCLOB that they were using the best technology available at the time.[159]

7. *The NSA should periodically review the types of communications acquired through "about" collection under Section 702, and study the extent to which it would be technically feasible to limit the types of "about" collection.* Again, the NSA conducted a review and concluded that no changes were practical at the time of the review.[160]

8. *To the extent consistent with national security, the government should create and release declassified versions of the minimization procedures of the NSA, CIA, and FBI.* All three agencies have released their current minimization procedures.[161]

9. *The government should implement five measures to provide insight about the extent to which the NSA acquires the communications involving US person and people located in the US under the Section 702 program.* The NSA will report statistics substantially similar to those requested by the Board.[162]

10. *The government should develop a methodology for assessing the value of counterterrorism programs.*[163] The Office of the Director of National Intelligence (ODNI) has advised the Board that it is working on this initiative.[164]

[92] Finally, in considering both the operation of Section 702 and the independence of the PCLOB, the Board, after receiving classified briefings on Section 702, came to this conclusion as part of its 196-page report:

---

[158] *Id.* at 12, 142-43.
[159] *Id.* at 12, 143-44.
[160] *Id.* at 13, 144-45.
[161] *Id.* at 13, 145-46. To view the 2015 NSA, CIA, and FBI minimization procedures, *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Release of 2015 Section 702 Minimization Procedures*, IC ON THE RECORD (Aug. 11, 2016) https://icontherecord.tumblr.com/post/148797010498/release-of-2015-section-702-minimization.
[162] *Id.* at 13, 146-147.
[163] *Id.* at 13, 148.
[164] *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, RECOMMENDATIONS ASSESSMENT REPORT, 26-27 (Jan. 29, 2015), https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf.

> 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.[165]

D. The Federal Privacy Council and Privacy and Civil Liberties Offices in the Agencies

[93] The US government has continued to expand the role of privacy and civil liberties offices in federal agencies. The Office of the Director of National Intelligence, which oversees the intelligence community, has the Office of Civil Liberties, Privacy, and Transparency.[166] In 2014, in connection with President Obama's speech on surveillance reform, the NSA appointed a Civil Liberties and Privacy Officer for the first time.[167] Other agencies have similar positions.[168] These offices have become centers of expertise within their agencies and a point of contact for those outside of their agencies who have privacy concerns.[169]

[94] In February 2016, President Obama issued Executive Order 13,719, establishing a Federal Privacy Council for US government agencies.[170] The Office of the Director for National Intelligence is one of the agencies designated to sit on the Council. The mission of the Council is

> to protect privacy and provides expertise and assistance to agencies; expand[] the skill and career development opportunities of agency privacy professionals; improve[] the management of agency privacy programs by identifying and sharing lessons learned and best practices; and promote[] collaboration between and among agency privacy professionals to reduce unnecessary duplication of efforts and to ensure the effective, efficient, and consistent implementation of privacy policy government-wide.[171]

---

[165] PCLOB 702 REPORT, *supra* note 78, at 2.
[166] OFFICE OF CIVIL LIBERTIES, PRIVACY AND TRANSPARENCY, *Who We Are*, DNI.GOV, http://www.dni.gov/clpo.
[167] President Obama issued PPD-28 on January 17, 2014. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform 2015 Anniversary Report*, IC ON THE RECORD (2015), http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#section-215. The US government announced the NSA's first CLPO on January 29, 2014. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *NSA Announces New Civil Liberties and Privacy Officer*, IC ON THE RECORD (Jan. 29, 2014), https://icontherecord.tumblr.com/post/75500428895/nsa-announces-new-civil-liberties-and-privacy.
[168] *See* PPD-28, *supra* note 141, at § 4(c).
[169] 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); DOJ Office of Privacy and Civil Liberties (http://www.justice.gov/opcl); and the 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 the Department of Defense Intelligence Oversight (http://dodsioo.defense.gov/Home.aspx).
[170] Exec. Order No. 13719 – Establishment of the Federal Privacy Council, 81 Fed. Reg. 29, 7685-89 (Feb. 9, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-02-12/html/2016-03141.htm.
[171] *Id.*

In addition to these agency-internal officers, an extensive oversight system exists within and across US executive agencies to report compliance incidents to the Foreign Intelligence Surveillance Court.[172]

V. Transparency Mechanisms

[95] There are numerous transparency safeguards in the system of US foreign intelligence law, including: federal agency reports on the number and type of surveillance orders; company transparency reports on such orders; provisions in the USA FREEDOM Act that require transparency of new legal decisions by the FISC; and new policies for transparency to the extent possible for FISC opinions. Since the Snowden disclosures, the US government, including by statute in the USA FREEDOM Act, has focused on increased transparency measures, both for companies subject to orders and for government agencies that have requested orders.[173] My research into the practices of other countries has found nothing close to the level of transparency and detail for the foreign intelligence surveillance practices of other countries.

A. Greater Transparency by the Executive Branch about Surveillance Activities

[96] Since 2013, the executive branch has undertaken a major transparency initiative in connection with the FISC and foreign intelligence more broadly. In its January 2015 report on Signals Intelligence Reform, the government reported eight categories of greater transparency that it had undertaken to that point,[174] and its 2016 report lists eight additional "specific transparency efforts" undertaken more recently.[175] Compared to the secrecy that historically had applied to signals intelligence, the shift toward greater transparency is remarkable, such as:

1. The declassification of numerous FISC decisions, discussed in more detail in Chapter 5;[176]

2. A new website devoted to public access to intelligence community information;[177]

---

[172] For a detailed discussion of the system of FISC compliance reporting, *see* Chapter 5, Section II(A).
[173] USA FREEDOM Act, Pub. L. No. 114-23, §§ 603, 604 (2015) (codified at 50 U.S.C. § 1874); *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2013*, IC ON THE RECORD (June 26, 2014), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.
[174] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform 2015 Anniversary Report*, IC ON THE RECORD (2015), http://icontherecord.tumblr.com/ppd-28/2015/enhancing-transparency.
[175] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform 2016 Progress Report*, IC ON THE RECORD (2016), https://icontherecord.tumblr.com/ppd-28/2016.
[176] As Jameel Jaffer, who was the Deputy Legal Director of the ACLU at the time of his comments and is currently the Director of the Knight First Amendment Institute at Columbia University, noted in his 2014 blog, the FISC began efforts to release opinions, transcripts, and briefs prior to the passage of the USA FREEDOM Act. Jameel Jaffer, *There Will Be Surveillance Reform*, JUSTSECURITY.COM (Nov. 20, 2014), https://www.justsecurity.org/17622/surveillance-reform/. This transparency effort by the FISC is discussed in detail in Chapter 5.
[177] IC ON THE RECORD, http://icontherecord.tumblr.com.

3. The first "Principles of Intelligence Transparency for the Intelligence Community;[178]

4. The first two Intelligence Community Statistical Transparency Reports;[179]

5. Unclassified reports on the NSA's implementation of Section 702[180] and its "Civil Liberties and Privacy Protections for Targeted SIGINT Activities";[181] and

6. 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.[182]

B. USA FREEDOM Act Provisions Mandating Public Law about Major FISC Decisions

[97] The USA FREEDOM Act contained a statutory transparency approach that I proposed in the 2004 article: When the FISC issues a "decision, order, or opinion" that contains "a significant construction or interpretation of any provision of law," FISA now requires the US government to (1) "conduct a declassification review" and (2) make the FISC decision "publicly available" to the greatest practicable extent.[183] In keeping with prior FISC practice, the government may redact national-security information from the FISC opinion prior to publication.[184]

[98] If the government asserts that an opinion must be withheld in full to protect national security or "intelligence sources or methods," the government must still provide an unclassified public summary of the FISC decision.[185] The summary must include (1) "to the extent consistent with national security, a description of the context in which the matter arises," as well as (2) "any significant construction or interpretation of any statute, constitutional provision, or other legal

---

[178] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, PRINCIPLES OF INTELLIGENCE TRANSPARENCY FOR THE INTELLIGENCE COMMUNITY (2015), https://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, PRINCIPLES OF INTELLIGENCE TRANSPARENCY IMPLEMENTATION PLAN (2015), https://www.dni.gov/index.php/newsroom/reports-and-publications/207-reports-publications-2015/1274-principles-of-intelligence-transparency-implementation-plan.

[179] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2014*, IC ON THE RECORD (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

[180] NSA DIR. OF CIVIL LIBERTIES AND PRIVACY OFFICE, NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 (Apr. 16, 2014), https://www.nsa.gov/about/civil-liberties/reports/.

[181] NSA DIR. OF CIVIL LIBERTIES AND PRIVACY OFFICE, NSA'S CIVIL LIBERTIES AND PRIVACY PROTECTIONS FOR TARGETED SIGINT ACTIVITIES UNDER EXECUTIVE ORDER 12333 (Oct. 7, 2014), https://www.nsa.gov/about/civil-liberties/reports/.

[182] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform, 2015 Anniversary Report – Enhancing Transparency*, https://icontherecord.tumblr.com/ppd-28/2015/enhancing-transparency.

[183] *See* 50 U.S.C. § 1872(a)-(b).

[184] *See id.* § 1872(b).

[185] *Id.* § 1872(c)(1).

authority relied on by the decision."[186] These provisions are designed to avoid any semblance of a 'secret court' and to ensure that FISC legal reasoning is consistently presented to the public.

C. The FISC and Numerous Opinions Declassified at IC on the Record

[99] Since 2013, based on my personal knowledge, the administration has made an energetic effort to review FISC opinions in order to declassify to the extent consistent with national security. The Office of the Director of National Intelligence maintains a website, accessible to the public, which contains declassified opinions of the FISC and its reviewing body, the Foreign Intelligence Court of Review.[187] This website is called "IC on the Record" and is located at https://icontherecord.tumblr.com/. This is a degree of transparency that few courts, and practically no other surveillance oversight bodies I am aware of, have achieved.

D. Transparency Reports by the US Government

[100] On its own initiative, as just discussed, the administration adopted a range of transparency reforms after 2013. The USA FREEDOM Act codified expansion in the annual reporting by the US government about its national security investigations.[188] Each year, the government is required to report statistics publicly for each category of investigation. Specifically, the government is required to report to Congress, and make publicly available: (1) a report on applications for tangible things under Section 215, to include requests for call detail records and the number of orders issued approving such requests; (2) a report on the total number of applications filed and orders issued under Section 702 as well as the estimated number of targets affected by such orders, to include the PRISM and upstream collection programs; and (3) a list of individuals appointed as *amici curiae* as well as any findings that an appointment was not appropriate.[189] The plain language of the statute thus provides that the US government will report annually on how many total targets have been affected.

[101] 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 time.

[102] Consistent with the requirements for statistical transparency, the US intelligence community now releases an annual Statistical Transparency Report,[190] with the statistics subject to oversight from Congress, Inspectors General, the FISC, the PCLOB, and others.[191] For 2015, there were 94,368 "targets" under the Section 702 programs, each of whom was targeted based on a finding of foreign intelligence purpose.[192] That is a tiny fraction of US, European, or global

[186] *Id.* § 1872(c)(2)(A).
[187] Any additional appeals would be taken to the United States Supreme Court.
[188] USA FREEDOM Act, Pub. L. No. 114-23, § 603 (2015).
[189] *Id.* §§ 601-602 (2015).
[190] Transparency reports have been released for every year since 2013.
[191] For a listing of the multiple oversight entities, *see* REVIEW GROUP REPORT, *supra* note 36, Appendix C at 269.
[192] The statistical reports define "target" in detail, and my assessment is that the number of individuals targeted is lower than the reported number.

Internet users. It demonstrates the low likelihood of the communications being acquired for ordinary citizens.[193]

E. Transparency Reports by Companies

[103] In recent years, companies that receive foreign intelligence orders from the government can publish considerably more detail about those orders. Five leading technology companies – Facebook, Google, LinkedIn, Microsoft, and Yahoo – filed suit in 2013 against the US government to be allowed to publish information about court orders they were receiving.[194] The DOJ changed its policy in January 2014 to permit companies to report ranges of the numbers of orders they receive.[195] For the first time, companies could report ranges of "[t]he number of FISA orders for content," as well as "[t]he number of customer selectors targeted under FISA content orders"[196] – both of which had been at the center of public debate following the disclosure of the PRISM program. Additionally, companies could report ranges of numbers on (1) the "number of NSLs (National Security Letters) received" and the "number of customer accounts affected by NSLs; (2) the "number of FISA orders for non-content" and the "number of customer selectors targeted" thereunder; or (3) "the total number of all national security process received, including all NSLs and FISA orders," along with the "total number of customer selectors targeted" through all such requests.[197]

[104] The USA FREEDOM Act codified and expanded the ability of companies to publish information in their transparency reports about categories of orders to which they replied. Companies now have four statutorily-guaranteed approaches by which they can provide statistics on orders for user information, and can do so – at their option – annually or semiannually.[198] Companies can report ranges of numbers of (1) National Security Letters, (2) FISA orders or directives, or (3) non-content requests – along with the "number of customer selectors" targeted under each such request.[199] Notably, they may continue to report ranges of the "total number of

---

[193] The 2016 *Statistical Transparency Report* reiterates the targeted nature of the surveillance: "Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information." OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2015*, IC ON THE RECORD, at "Response to PCLOB Recommendation 9(5)" (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

[194] *See* Mot. for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders, *In re Motion for Declaratory Judgment of Google, Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, No. Misc. 13-03 (F.I.S.C. June 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-10.pdf; Microsoft Corp.'s Mot. for Declaratory Judgment or Other Appropriate Relief Authorizing Disclosure of Aggregate Data Regarding Any FISA Orders It Has Received, *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, No. Misc. 13-04 (F.I.S.C. June 19, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-04%20Motion-10.pdf.

[195] *See* Letter dated January 27, 2014 from James M. Cole, US Deputy Attorney General, Dep't of Justice, to General Counsels of Google, Microsoft, Yahoo, Facebook, and LinkedIn, https://www.justice.gov/iso/opa/resources/422201412716042240387.pdf (proposing settlement terms for each company's respective legal action then pending in the F.I.S.C.).

[196] *See id.*

[197] *See id.*

[198] USA FREEDOM Act, Pub. L. No. 114-23, § 604 (2015) (codified at 50 U.S.C. § 1874(a)).

[199] *See* 50 U.S.C. § 1874(a)(1).

all national security process received" – including National Security Letters and FISA orders and directives – as well as the number of customers affected by such requests.[200]

[105] In my view, these statistics provide important evidence about the actual scope of national security investigations in the US. I have examined the most recent transparency reports of Facebook and Google, and the percentage of users whose records are accessed in the most recent six-month period is vanishingly small. 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 no more than (1) 18,000[201] for Facebook, out of approximately 1.5 billion[202] active users per month; and (2) approximately 15,000[203] for Google, out of approximately 1.17 billion[204] active users per month.

Facebook	# of Users Accessed in 6 months	Percentage based on Users Per Month
Non-Content Requests	0-499	.00003%
Content Requests	13,500-13,999	.00093%
National Security Letters	0-499	.00003%

Google	# of Users Accessed in 6 months	Percentage based on Users Per Month
Non-Content Requests	0-499	.00004%
Content Requests	16,000-16,499	.00141%
National Security Letters	500-999	.00009%

[106] These statistics indicate that Google and Facebook, and their customers, are not subject to 'pervasive' surveillance. If one assumes that everyone within the 1.1 million population of Dublin and its suburbs[205] is a Google user, no more than 15 users would on average be affected by content requests. No more than two users on average would be affected by non-content requests or national

[200] *See id.* § 1874(a)(3). If companies elect to report annually instead of semi-annually, they may report the total number of all national security process in bands of 100. *See id.* § 1874(a)(4).
[201] 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 January 2015 - June 2015, Facebook received the following: 0-499 non-content requests; 13,500-13,999 content requests; and 0-499 national security letters. *See* FACEBOOK, *United States Law Enforcement Requests for Data*, GOVERNMENT REQUESTS REPORT (2016), https://govtrequests.facebook.com/country/United%20States/2015-H1.
[202] *See* STATISTA, *Number of Monthly Active Facebook Users Worldwide as of 2nd Quarter 2016* (2016), http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.
[203] For the time period from January 2015 - June 2015, Google received the following: 0-499 non-content requests; 16,000-16,499 content requests; and 500-999 national security letters. *See* GOOGLE, *Transparency Report – United States* (2016), https://www.google.com/transparencyreport/userdatarequests/US/.
[204] *See* Craig Smith, *100 Google Search Statistics and Fun Facts*, EXPANDEDRAMBLINGS.COM (Oct. 19, 2016), http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts.
[205] CENTRAL STATISTICS OFFICE, PROFILE 1 TOWN AND COUNTRY, 11 (Apr. 2012) (Ir.), http://www.cso.ie/en/media/csoie/census/documents/census2011vol1andprofile1/Profile1_Town_and_Country_Entire_doc.pdf.

security letters. It seems a mischaracterization to count 17 users out of over one million people as "mass and indiscriminate" surveillance.

VI. Executive Branch Safeguards

[107] This Chapter has already discussed the many systemic safeguards created by statute in the US and has described existing oversight and transparency mechanisms. This section discusses some of the other safeguards, especially those adopted since 2013, which apply within the executive branch.

[108] The section begins with observations on reasons to believe that US agencies indeed follow these executive branch safeguards. It next discusses Presidential Policy Directive 28 in some detail, because of the range of safeguards announced in it by President Obama. The discussion here addresses six aspects of PPD-28: (1) a principle to protect the privacy rights of non-US persons in signals intelligence; (2) protection of civil liberties in addition to privacy; (3) minimization requirements in collection of signals intelligence; (4) dissemination and retention limits for signals intelligence; (5) limits on bulk collection of information; and (6) limits on surveillance to gain trade secrets for commercial advantage.

[109] The discussion then turns to other executive branch safeguards that have come into existence since 2013: (1) a new White House oversight of sensitive intelligence collection, including of foreign leaders; (2) a new White House process to help fix software flaws rather than use them for surveillance; (3) the apparently imminent separation of US Cyber Command from the NSA; (4) the Umbrella Agreement as a systemic safeguard; and (5) the Privacy Shield as a systemic safeguard.

A. Do the Agencies Follow the Safeguards?

[110] Before discussing the specific safeguards, I offer some observations more generally, based on my experience, about the extent to which legal safeguards are followed within the US government, and in the intelligence community in particular. In talking with people outside of the US government, including during my trips to Europe, I have sometimes encountered skepticism about whether agencies follow the rules, including for surveillance activities. This skepticism is fueled, in my view, by inaccurate television and other media portrayals of intelligence activities – sometimes it seems in every episode of a show that a character says he or she has to break the rules to get the bad guy. Jack Bauer in the television show "24" or similar characters, always breaking the rules, may make for exciting drama, but it is bad social science.

[111] My overall experience, from two decades of working in and with employees and contractors for the US government, is much less cynical. My experience is that the rules matter a great deal in practice, so that the creation of new safeguards directly affects how the agencies act. The legal culture in the US often favors enforcement, such as the Federal Trade Commission vigorously enforcing against "deceptive" trade practices, defined as when an organization breaks its own privacy promises. We have seen public examples of this enforcement in the privacy context. For instance, in the so-called "LOVEINT" cases, a handful of NSA employees improperly accessed information about individuals they knew, and were sanctioned or voluntarily left their

employment before a sanction was imposed on them.[206] Similarly, the clear policy in the Internal Revenue Service has been to fire employees who improperly access the records of celebrities or people they know.[207]

[112] The Review Group, after its investigations based on access to top-secret materials, had a positive view about the NSA's pattern of following the law and executive branch rules. The Report stated: "NSA employs large numbers of highly trained, qualified, and professional staff. The hard work and dedication to mission of NSA's work force is apparent. NSA has increased the staff in its compliance office and addressed many concerns expressed previously by the FISC and others."[208] In contrast to the period immediately after the attacks of September 11, 2001, when new programs were being put into place on an emergency basis, the NSA over time in its Section 215 and other programs built a substantial and effective compliance program. The rigor of the compliance efforts, including upgrades to the software to catch any violations, became greater after concerns stated by FISC judges in 2009, but that is exactly the point. There are multiple checks and balances built into the system, including a culture of following established rules, and audits, software, and other oversight mechanisms to catch violations.

[113] This pattern of following the rules is reinforced by the US government legal culture that applies today and in the foreseeable future concerning aggressive interpretations of surveillance authorities. Put simply, the aggressive interpretations that were allowed in the wake of September 11, 2001 would have little chance of being approved today. One reason is statutory. As discussed above in connection with the prohibition on bulk collection under the USA FREEDOM Act, Congress and the President approved legislation sending a clear signal against bulk collection. A second reason may be more subtle but equally powerful. In my years of research and government service on these issues, I spoke on a number of instances with people who lived through the Watergate scandal and the Church Commission. They told me that their friends and colleagues had lost jobs or had their careers harmed by participating in the aggressive practices that were revealed then. As a result, that generation of government employees appreciated the risks of breaking the rules, and were a voice for caution against rule-breaking. In the view of people I have interviewed, that generation had largely lost their influence in government by 2001, and the new decision makers were willing to be more aggressive in interpreting authorities.[209]

[114] The events since the Snowden disclosure, in my view, have created a new generation of lawyers and others in the agencies who are deeply aware of the risks of breaking the rules. As discussed in the Chapter 5, review by the FISC judges has become very tight, so lawyers for the agencies have good reason to be cautious in interpreting the scope of authorities. Individuals at the NSA and in other agencies also now realize, far more than before, that their secret activities may become public, so they have reason to resist being involved in any activities that would look

---

[206] *See* Evan Perez, *NSA: Some Used Spying Power to Snoop on Lovers*, CNN.COM (Sept. 27, 2013), http://www.cnn.com/2013/09/27/politics/nsa-snooping/.

[207] Peter Swire, *Peeping*, 24 BERKELEY TECH. L.J. 1164 (2009), http://peterswire.net/archive/Peeping.pdf.

[208] REVIEW GROUP REPORT, *supra* note 36, at 179.

[209] As an analogy, consider investment bankers who have worked only in a bull market but never experienced a crash or major downturn. My view is that those who have seen only the bull market are more willing to take chances, including breaking the rules. Those who have experienced the bad market are less willing to put their careers on the line by rule-breaking that will be discovered if a downturn occurs.

bad if disclosed.[210] In short, a culture of following the rules has been reinforced by the painful experience and criticism that the US intelligence community has gone through since 2013.

B. Presidential Policy Directive 28

[115] The Executive Branch has multiple safeguards in place to supplement legislative safeguards, including Presidential Policy Directive 28 (PPD-28), which creates an extensive system of privacy protection for signals intelligence activities, such as collection of electronic communications of non-US persons.[211] In 2014, President Obama issued PPD-28. The discussion here addresses six aspects of PPD-28: (1) a principle to protect the privacy rights of non-US persons in signals intelligence; (2) protection of civil liberties in addition to privacy; (3) minimization requirements in collection of signals intelligence; (4) dissemination limits for signals intelligence; (5) limits on bulk collection of information; and (6) limits on surveillance to gain trade secrets for commercial advantage. Because these safeguards apply to all signals intelligence, they update and modify earlier executive branch rules, such as Executive Order 12,333, which applies to intelligence collected outside of the US.[212]

---

[210] I discuss the increased likelihood of intelligence secrets becoming known, and the implications of that, in Peter Swire, *The Declining Half-Life of Secrets and the Future of Signals Intelligence*, NEW AMERICA (July 2015), https://static.newamerica.org/attachments/4425-the-declining-half-life-of-secrets/Swire_DecliningHalf-LifeOfSecrets.f8ba7c96a6c049108dfa85b5f79024d8.pdf.

[211] *See* PPD-28, *supra* note 141.

[212] I do not discuss Executive Order 12,333 in detail due to my understanding of the scope of the proceeding, which concerns the adequacy of safeguards against excessive surveillance in the event of transfer of personal data from the EU to the US. Executive Order 12,333 is "the principal Executive Branch authority for foreign intelligence activities *not governed by FISA*" and is, indeed, the "principal governing authority for United States intelligence activities *outside the United States*." *See* REVIEW GROUP REPORT, *supra* note 36, at 69-70 (emphasis in original). For data transfers, the US logically could collect the information in two ways. First, if the personal data is collected within the US, then collection is done, effectively, either under law enforcement authorities or foreign intelligence authorities, notably FISA. The materials I am submitting discuss in detail the systemic safeguards for law enforcement and foreign intelligence collection within the US.

Second, the personal data might be collected by the US in transit from the EU to the US, such as through access via undersea communications cables. The possibility of collection via cables is discussed in the Privacy Shield materials, in a letter from the US Office of the Director for National Intelligence, stating: "[W]ithout confirming or denying media reports alleging that the US Intelligence Community collects data from transatlantic cables while it is being transmitted to the United States, were the US Intelligence Community to collect data from transatlantic cables, it would do so subject to the limitations and safeguards set out herein, including the requirements of PPD28." EU-U.S. PRIVACY SHIELD, Annex VI, at 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL. The EU Commission analyzed this topic in its decision upholding the adequacy of the Privacy Shield. The Commission found PPD-28's protections embody "the essence of the principles of necessity and proportionality" because under PPD-28 "[t]argeted collection is clearly prioritised, while bulk collection is limited to (exceptional) situations where targeted collection is not possible for technical or operational reasons." Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, para. 76, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL.

Along with this recognition of the safeguards that apply to any US access to undersea cables, I offer additional observations based on my research into the growing prevalence of effective encryption for communications in transit, such as those transiting undersea cables. In 2016, I was lead author on a study showing rapid and continuing growth in the prevalence of strong encryption for Internet communications, with such encryption already being predominant for many applications, including emails and text messaging. This prevalent use of encryption makes it far more difficult than previously for those conducting surveillance to access the contents of communications. *See* Peter Swire, Testimony before the US Senate Commerce Committee on "How Will the

[116] I consider PPD-28 to be a historic document, announcing principles and practices to govern intelligence activities undertaken outside of the country. In its specificity and numerous provisions, PPD-28 goes beyond what other countries have announced in the intelligence field.

1. Privacy is Integral to the Planning of Signals Intelligence Activities

[117] 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.[213] Spying on hostile actors is especially understandable during time of war or when there is reason to believe hostile actors may attack.

[118] The US and the Member States of the EU 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.

[119] PPD-28 made it US government policy to respect the privacy of non-US persons in signals intelligence activities. Under PPD-28, "[p]rivacy and civil liberties shall be integral considerations in the planning of US signals intelligence activities."[214] It further states: "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."[215] Privacy issues do not overrule national security issues; instead, privacy is an integral part of the overall consideration of how to proceed.

FCC's Proposed Privacy Rules Affect Consumers and Competition?" (July 12, 2016), https://iisp.gatech.edu/sites/default/files/images/swire_commerce_fcc_privacy_comments_07_12_2016.pdf, (discussing encryption research).

To summarize, my Testimony and the accompanying Chapters explain in detail the systemic safeguards that apply to data collected in the US. Executive Order 12,333 applies to "intelligence activities outside the United States." REVIEW GROUP REPORT, *supra* note 36, at 70. This discussion of undersea cables explains the legal adequacy finding made by the Commission with respect to communications in transit. That legal adequacy is bolstered in practice by the shift toward pervasive use of encryption in transit.

[213] For a translation of *Ch. 13, The Use of Spies* in the 5th Century B.C.E. classic Chinese military treatise by SUN TZU, THE ART OF WAR, *visit* http://suntzusaid.com/book/13.

[214] PPD-28, *supra* note 141, at § 1(b); *see* also OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, SAFEGUARDING THE PERSONAL INFORMATION OF ALL PEOPLE: A STATUS REPORT ON THE DEVELOPMENT AND IMPLEMENTATION OF PROCEDURES UNDER PRESIDENTIAL POLICY DIRECTIVE 28, 5 (July 2014), https://fas.org/irp/dni/ppd28-status.pdf. This approach ensures that when the US conducts foreign surveillance, it takes into account, not only the nation's security requirements, but also the security and privacy concerns of the US's allies.

[215] PPD-28, *supra* note 141, at introductory statement.

2. Protection of Civil Liberties in Addition to Privacy

[120] PPD-28 protects civil liberties in addition to the protection of privacy. 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."[216] Similarly, 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. More specifically, "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."[217]

3. Minimization Safeguards

[121] 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 the extent consistent with classification requirements. By 2015, all intelligence agencies had completed new policies or revised existing policies to meet the President's mandates.[218]

[122] The policies and procedures address topics 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."[219]

[123] 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."[220] This quotation does not mention words from EU data protection law such as "necessary" and "proportionate," but being "as tailored as feasible," mandating use limits, and prioritizing alternatives to signals intelligence are some of many examples in US law where specific safeguards address those concerns.

---

[216] *Id.* § 1(b).
[217] *Id.*
[218] The NSA policies and procedures to protect personal information collected through SIGINT can be found at NATIONAL SECURITY AGENCY, PPD-28 SECTION 4 PROCEDURES (Jan. 12, 2015), https://www.nsa.gov/news-features/declassified-documents/nsa-css-policies/assets/files/PPD-28.pdf. Links to the policies and procedures for the ODNI, the CIA, the FBI, and other agencies can be found at: OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform 2015 Anniversary Report*, IC ON THE RECORD (2015), http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. Additional policies on the site include: National Reconnaissance Office, the Department of Homeland Security, the Drug Enforcement Administration, the State Department, the Treasury Department, the Department of Energy, the US Coast Guard, and Other IC Elements in the Department of Defense.
[219] PPD-28, *supra* note 141, at § 4(a).
[220] *Id.* § 1(d).

[124] The minimization requirements in PPD-28 supplement the minimization safeguards that exist under the other relevant aspects of US law, such as FISA generally, the Wiretap Act, and Sections 215 and 702.[221]

4. Retention, Dissemination, and Other Safeguards for Non-US Persons Similar to Those for US Persons

[125] The agency procedures put in place pursuant to Section 4 of PPD-28 have created new limits that address concerns about the retention and dissemination of signals intelligence. The new retention requirements and dissemination limitations are consistent across agencies and similar to those for US persons.[222] 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.[223] 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 US persons would be permitted."[224]

[126] 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."[225]

5. Limits on Bulk Collection of Signals Intelligence

[127] 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."[226]

---

[221] *See* NSA DIR. OF CIVIL LIBERTIES AND PRIVACY OFFICE, NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT (Apr. 16, 2014), https://www.nsa.gov/about/civil-liberties/reports/assets/files/nsa_report_on_section_702_program.pdf; 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); USA FREEDOM Act, Pub. L. No. 114-23, § 104 (2015).

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

[223] There are exceptions to the five-year limit, but they can only apply after the Director of National Intelligence considers the views of the ODNI's Civil Liberties Protection Officer and other agency privacy and civil liberties officials. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform 2015 Anniversary Report*, IC ON THE RECORD (2015), http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

[224] PPD-28, *supra* note 141, at § 4(a)(i).

[225] *Signals Intelligence Reform 2015 Anniversary Report*, *supra* note 223, at "Oversight, Training & Compliance Requirements."

[226] PPD-28 says: "The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection." *Supra* note 141, at § 2. The detailed rules governing targeted collection under Section 702 can be found in Chapters 3 and 5.

[128] PPD-28 announces purpose limitations – when the US collects non-publicly 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 US or allied Armed Forces or other US or allied personnel; and
(6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.

If this list is updated, it will be "made publicly available to the maximum extent feasible."[227]

6. Limits on Surveillance to Gain Trade Secrets for Commercial Advantage

[129] European and other nations have long expressed concern that US surveillance capabilities would be used for the advantage of US commercial interests. These concerns, if true, would provide an economic reason to object to US signals intelligence, in addition to privacy and civil liberties concerns.

[130] 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."[228] 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.

[131] The distinction in PPD-28 is that "[i]t is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to US companies and US business sectors commercially."[229] 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.[230]

---

[227] PPD-28, *supra* note 141, at § 2.
[228] *Id.* at § 1, (c).
[229] *Id.*
[230] The *Venice Commission Report* notes that five European countries – Ireland, Germany, the Netherlands, Sweden, and the UK – that are involved in signals intelligence allow such surveillance for economic well-being. The Commission cautions that the broad terms used as the basis for surveillance should be clarified, "as the applicable US regulations now do." European Commission for Democracy through Law (Venice Commission), UPDATE OF THE 2007 REPORT ON THE DEMOCRATIC OVERSIGHT OF THE SECURITY SERVICES AND REPORT ON THE DEMOCRATIC OVERSIGHT OF SIGNALS INTELLIGENCE AGENCIES, para. 77 (April 7, 2015), http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e; *see European Union Agency for Fundamental Rights Report*, *supra* note 104, at 26 (2015).

7. Discussion of PPD-28

[132] These specific safeguards under PPD-28 are accompanied by transparency and other provisions to assure the proper handling of information related to non-US persons. For transparency purposes, PPD-28 requires intelligence agencies to publicly release their implementation procedures, to the maximum extent feasible that is consistent with requirements concerning classified documents.[231] The procedures adopted by the NSA, CIA, and FBI are available online.[232]

[133] To ensure that foreign intelligence programs are as tailored as feasible, executive agencies are required, where practicable, to focus collection on specific foreign intelligence targets through the use of discriminants – such as selectors and identifiers.[233] To protect civil liberties and privacy, executive agencies are required to consult with agency officials responsible for civil liberties and privacy to ensure appropriate safeguards for a new program is undertaken or a significant change is made to an existing program.[234]

[134] According to PPD-28, agency privacy and civil liberties officers, in conjunction with the Office of the Director of National Intelligence's Civil Liberties and Privacy Office, will periodically review the compliance of these agencies with their procedures.[235] In addition, the procedures must also require that any significant compliance issues involving any person, regardless of nationality, be promptly reported to the head of the intelligence agency; that agency head must then promptly report the incident to the Director of National Intelligence (DNI). If the issues involve a non-US person, the DNI is required to consult with the US Secretary of State to determine whether to notify the relevant foreign government.[236]

[135] 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 the US. PPD-28 is binding upon executive branch agencies as an instruction from the head of the executive branch, even if it cannot be enforced by outsiders. Within the military, including for military personnel in the NSA, PPD-28 has the effect of an order from the Commander-in-Chief. 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.

---

[231] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, SAFEGUARDING THE PERSONAL INFORMATION OF ALL PEOPLE: A STATUS REPORT ON THE DEVELOPMENT AND IMPLEMENTATION OF PROCEDURES UNDER PRESIDENTIAL POLICY DIRECTIVE 28, 2-9 (July 2014), https://fas.org/irp/dni/ppd28-status.pdf.

[232] NAT'L SEC. AGENCY, PPD-28 SECTION 4 PROCEDURES (Jan. 12, 2015), https://www.nsa.gov/news-features/declassified-documents/nsa-css-policies/assets/files/PPD-28.pdf; CENT. INTELLIGENCE AGENCY, SIGNALS INTELLIGENCE ACTIVITIES (undated), https://www.dni.gov/files/documents/ppd-28/CIA.pdf; FED. BUREAU OF INVESTIGATION, PRESIDENTIAL POLICY DIRECTIVE 28 POLICIES AND PROCEDURES (Feb. 2, 2015), https://www.dni.gov/files/documents/ppd-28/FBI.pdf.

[233] SAFEGUARDING THE PERSONAL INFORMATION OF ALL PEOPLE, *supra* note 219, at 4.

[234] *Id.* at 3-4.

[235] *Id.* at 8.

[236] *Id.* at.7.

C. New White House Oversight of Sensitive Intelligence Collection, including of Foreign Leaders

[136] Based on our work in the Review Group, in the aftermath of the attacks of September 11, 2001, my view is that intelligence agencies sometimes have 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.

[137] The Obama Administration accepted the Review Group recommendation to create a stricter procedure to assess sensitive intelligence collection, as part of the National Intelligence Priorities Framework.[237] 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.[238] 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."[239]

[138] The new oversight process supports the PPD-28 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."[240] Potential damage cited in PPD-28 includes compromise of intelligence sources and methods, as well as harm to diplomatic relationships and other interests.

[139] 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."[241]

D. New White House Process to Help Fix Software Flaws, rather than Use Them for Surveillance

[140] Going beyond traditional rules about the scope of intelligence, the Review Group made other recommendations that affected overall foreign intelligence practices, such as the approach to "Zero Day" attacks. The Review Group recommended a new process to evaluate what to do with

---

[237] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform 2015 Anniversary Report*, IC ON THE RECORD (2015), http://icontherecord.tumblr.com/ppd-28/2015/limiting-sigint-collection.
[238] *Id.*
[239] *Id.*
[240] PPD-28, *supra* note 141, at § 3.
[241] President Barack Obama, Remarks by the President on Review of Signals Intelligence, WHITEHOUSE.GOV, OFFICE OF THE PRESS SEC'Y (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

so-called "Zero Day" attacks, where software developers and system owners have zero days to address and patch the vulnerability.[242] 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.

[141] Previously, the decision was made within 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) versus for defense (to patch our own networks). In 2014, the White House announced that the White House itself would lead what it called a "disciplined, rigorous and high-level decision-making process for vulnerability disclosure."[243] In my view, this new inter-agency process, chaired by the President's Cybersecurity Coordinator, improves on the old system conducted inside the NSA. The new process brings in perspectives from more stakeholders, such as the Departments of Commerce and State, 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.

E. The Umbrella Agreement as a Systemic Safeguard

[142] The Umbrella Agreement, which the EU and US entered into in 2016, is discussed in greater detail in Chapter 7. I mention it briefly here to point out that the Agreement serves as a systemic safeguard on how data is used once transferred to the US.

[143] The Umbrella Agreement provides a data protection framework for personal data exchanged between the EU and the US for the purposes of prevention, detection, investigation, and prosecution of crimes. The agreement specifically includes terrorism within the crimes that it covers.[244] Important aspects of the Agreement include: (1) limiting the usage of data to that related to addressing criminal activity; (2) restricting onward transfer of the data to instances where prior consent is obtained from the country that initially provided the data; (3) requiring retention periods for the data obtained to be made public; and (4) providing the individual to whom the data refers the right to access and rectify any inaccuracies.[245] Along with the individual remedy, the limits on use, onward transfer, and retention are systemic safeguards for the handling of data transferred to the US.

---

[242] REVIEW GROUP REPORT, *supra* note 36, at 219.

[243] Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, WHITEHOUSE.GOV (Apr. 28, 2014), https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

[244] Press Statement, Dep't of Justice, Joint EU-U.S. Press Statement Following the EU-U.S. Justice and Home Affairs Ministerial Meeting (June 2, 2016), https://www.justice.gov/opa/pr/joint-eu-us-press-statement-following-eu-us-justice-and-home-affairs-ministerial-meeting; European Commission Press Release MEMO/15/5612, Questions and Answers on the EU-US data protection "Umbrella agreement" (Sep. 8, 2015), http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm. Both the US and EU Member States engage in national security surveillance programs that involve data transfers. These programs are specifically excluded from the Umbrella Agreement.

[245] *Communication from the Commission to the European Parliament and the Council, Transatlantic Data Flows: Restoring Trust through Strong Safeguards*, at 12-13, COM (2016) 117 final (Feb. 29, 2016), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

F. Privacy Shield as a Systemic Safeguard

[144] The Privacy Shield is discussed in greater detail in Chapter 7, where I provide details about the remedies individuals have against the US government, notably through the Ombudsman, and against companies participating in the Privacy Shield. That discussion also points out that the US government's commitments apply to other lawful bases for data transfers from the EU to the US, such as under Standard Contractual Clauses.

[145] Along with enforcement concerning individual complaints, the Privacy Shield includes commitments from the US government generally, and the US Department of Commerce and the FTC in more detail, to act promptly and effectively to address EU data protection concerns. Along with the safeguards provided through those agencies, there is an annual review process. These commitments and reviews provide the EU and its DPAs with an ongoing mechanism to protect personal data transferred to the US, including data processed for national security purposes.

VII. Conclusion

[146] This lengthy Chapter has summarized the numerous systemic safeguards that exist in the US to govern foreign intelligence investigations. Chapter 4 summarizes the systemic safeguards that exist for law enforcement investigations. Chapter 7 summarizes the remedies available to individuals, notably EU persons, in the US. Chapter 6 assesses the US protections under the criteria for surveillance safeguards developed by Oxford Professor Ian Brown and colleagues. The Brown study shows that the US has more complete safeguards than other countries.

[147] Intelligence agencies necessarily often act in secret, to detect intelligence efforts from other countries and for compelling national security reasons. The US has developed multiple ways to create transparency without compromising national security, and oversight by persons with access to classified information for the necessarily secret activities. These systemic safeguards, in my view, provide effective checks against abuse of secret surveillance powers.