TESTIMONY OF PROFESSOR PETER SWIRE

TABLE OF CONTENTS

CHAPTER 1:
SUMMARY OF TESTIMONY

CHAPTER 2:
BIOGRAPHICAL CHAPTER OF PETER SWIRE

CHAPTER 3:
SYSTEMIC SAFEGUARDS IN THE US SYSTEM OF FOREIGN INTELLIGENCE SURVEILLANCE LAW

CHAPTER 4:
SYSTEMIC SAFEGUARDS FOR LAW ENFORCEMENT

CHAPTER 5:
THE US FOREIGN INTELLIGENCE SURVEILLANCE COURT

CHAPTER 6:
COMPARISON CRITERIA DEVELOPED BY THE OXFORD TEAM

CHAPTER 7:
INDIVIDUAL REMEDIES IN US PRIVACY LAW

CHAPTER 8:
INDIVIDUAL REMEDIES, HOSTILE ACTORS, AND NATIONAL SECURITY CONSIDERATIONS

CHAPTER 9:
THE BROAD SCOPE OF "ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS" SUBJECT TO SECTION 702

CHAPTER 1:

SUMMARY OF TESTIMONY

INTRODUCTION

[1] This Chapter is a Summary of Testimony, with many of the points developed in greater detail in the accompanying Chapters 2 to 9. I understand that my duty as an expert is to assist the Court as to matters within my area of expertise and this overrides any duty or obligation that I may owe to the party whom I have been engaged by or to any party liable to pay my fees.

[2] In this Chapter, Part 1 gives a summary of my experience related to the matters before the Court, as a privacy expert for over two decades, with particular focus on both United States (US) surveillance law and European Union (EU) data protection law. It notes my history of scholarly critique of US surveillance practices.

[3] Part 2 summarizes the system of safeguards in US law and practice that protect all persons, both in and out of the US. These numerous safeguards are described in detail in Chapters 3 and 4, and include multiple oversight bodies and transparency requirements, as well as judicial review of foreign intelligence investigations. Intelligence agencies necessarily often need to act in secret, to detect intelligence efforts from other countries and for compelling national security reasons. The US has developed multiple ways to ensure oversight by persons with access to classified information for the necessarily secret activities, and to create transparency in ways that do not compromise national security.

[4] The systemic safeguards discussed in Part 2 include:

1. 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;

2. The systemic statutory safeguards governing foreign intelligence surveillance;
3. The oversight mechanisms;

4. The transparency mechanisms; and

5. Administrative safeguards that are significant in practice and supplement the legislative safeguards.

[5] In my view, the US system overall provides effective safeguards against abuse of secret surveillance powers. I agree with the team led by Oxford Professor Ian Brown, who after comparing US safeguards to other countries, concluded that "the US now serves as a baseline for foreign intelligence standards," and that the legal framework for foreign intelligence collection in the US contains clearer rules on collection, use, sharing and oversight of data relating to foreign nationals than the laws of almost all EU Member States.[1] In addition, as shown in the analysis of the Foreign Intelligence Surveillance Court in Chapter 5, those rigorous legal standards are

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

effectively implemented in practice, under the supervision of independent judges with access to top-secret information. In addition, these systemic safeguards in the foreign intelligence realm are complemented by safeguards in the criminal procedure realm that in significant respects are stricter than EU Member States.

[6] Part 3 describes how individuals (including residents of EU Member States) have access to multiple remedies in the US for violations of privacy. It outlines the paths an aggrieved person in the US or resident of an EU Member State may take in response to concerns regarding US privacy violations:

1. I discuss individual judicial remedies against the US government, including the recently-finalized Privacy Shield and Umbrella Agreement, as well as the recently passed Judicial Redress Act.

2. I examine the civil and criminal remedies available in the event that individuals, including government employees, violate wiretap and other surveillance rules under laws such as the Stored Communications Act, the Wiretap Act, and the Foreign Intelligence Surveillance Act.

3. I highlight three paths of non-judicial remedies any individual in the US or EU can take: the Privacy and Civil Liberties Oversight Board, Congressional committees, and recourse to the US free press and privacy-protective non-governmental organizations.

4. I analyze individual remedies against US companies that improperly disclose information to the US government about customers or other persons. These causes of action against US companies can be brought both by individuals (US and non-US) as well as by US federal administrative agencies.

5. I also examine remedies available under state law in the US, including enforcement by state Attorneys General, as well as private rights of action, which are generally far easier to bring in the US than in the EU.

[7] **In summary on Parts 2 and 3, the combination of systemic safeguards and individual remedies in the US, in my view, are effective and "adequate" in safeguarding the personal data of non-US persons. Moreover, the Court of Justice of the European Union (CJEU) has announced a legal standard of "essential equivalence" for transfers of personal data to third countries such as the US. Based on my comprehensive review of US law and practice, and my years of experience in EU data protection law, my conclusion is that overall intelligence-related safeguards for personal data held in the US are greater than in EU Member States. Even more clearly, the US safeguards are at least "essentially equivalent" to EU safeguards. I therefore do not see a basis in law or fact for a conclusion that the US lacks adequate protections, due to its intelligence activities, for personal data transferred to the US from the EU.**

[8] Part 4 discusses the potentially very broad impact were the EU to find a lack of "adequacy" or "essential equivalence." The following are key conclusions, which I reach based on the analysis in this and accompanying chapters:

1. US law defines the term "electronic communications service provider" broadly to include any company providing an email or similar communication system. A finding of inadequacy would apply to the full set of such providers. The effect of this proceeding on companies doing business in both the US and EU is thus potentially very broad.

2. The surveillance safeguards in most or all other countries outside the EU are less extensive than those in the US. The effect of an inadequacy finding would thus logically appear to apply to transfers to all non-EU countries, except any whose safeguards against surveillance are greater than those in the US.

3. An inadequacy finding for Standard Contract Clauses may have implications for other lawful bases for data transfers. I make no statement about whether a finding of inadequacy for SCCs would entail a finding of inadequacy for Privacy Shield or Binding Corporate Rules. The discussion here does support the possibility of a "categorical finding of inadequacy" – a finding of inadequacy that would apply not only to SCCs but also to Privacy Shield and BCRs. A categorical finding of inadequacy would have significant implications for the overall EU/US relationship, affecting the foreign relations, national security, economic, and other interests of the Member States and the EU itself.

4. This Testimony supports the conclusion that an inadequacy finding would have large effects on EU economic well-being. EU institutions and Member States have clearly indicated the economic importance of maintaining data flows with the US. In addition, the General Agreement of Trade in Services bans "discrimination between countries where like conditions prevail." There appears to be a strong case that such discrimination would exist if transfers to the US were barred, despite less extensive surveillance safeguards in most non-EU nations and EU Member States themselves.

5. A finding of inadequacy would also create large risks for EU national security and public safety. NATO and other treaty obligations emphasize information sharing for national security purposes. The EU has stated that EU/US information sharing is "critical to prevent, investigate, detect and prosecute criminal offenses, including terrorism."

[9] In summary, the combination of systemic safeguards and individual remedies in the US, in my view, are effective and "adequate" in safeguarding the personal data of non-US persons. These actions are necessary and taken in accordance with law. In light of those safeguards and individual remedies available to EU citizens in connection with data transferred to the US, I respectfully believe and assert that continued transfers of personal data under Standard Contract

Clauses are necessary in a democratic society to protect vital interests of the EU, including national security, public safety, and economic well-being.

PART 1:
Biographical Summary for Peter Swire

[10] My overall expertise in privacy has developed through more than 20 years of focusing primarily on privacy and cybersecurity issues, as both a professor and senior government official.[2] I have written six books and numerous academic articles, and have testified before a dozen committees of the US Congress. I am lead author of the standard textbook used for the US private-sector privacy examination of the International Association of Privacy Professionals (IAPP).[3] In 2015, the IAPP, among its over 20,000 members, awarded me its Privacy Leadership Award.

[11] For government service, under President Bill Clinton I was Chief Counselor for Privacy in the US Office of Management and Budget, the first person to have US government-wide responsibility for privacy issues. Under President Barack Obama, I was Special Assistant to the President for Economic Policy in 2009-10. In 2013, after the initial Snowden revelations, President Obama named me as one of five members of the Review Group on Intelligence and Communications Technology (which I refer to as the "Review Group").

[12] To the best of my knowledge, I am the only person to have authored both a book on EU data protection law as well as one on US surveillance law. In Chapter 2, I highlight my experiences in both areas, including how these experiences have informed and shaped my views on these issues over more than two decades.

[13] My views on the overall adequacy of protections related to US surveillance practices have changed a great deal over time, in light of pro-privacy reforms that the US has adopted. In 2004, my law review article on "The System of Foreign Intelligence Law" criticized multiple aspects of the US regime.[4] Approximately 10 recommendations from that paper have now become the law and practice in the US, as shown in the Annex to Chapter 2. Many additional reforms have occurred since 2013, as discussed in my 2015 Testimony for the Belgium Privacy Agency.[5] Based on these reforms, and my study of the systems in other countries, my assessment of the US system has developed to one in line with the Oxford team that finds the US to be the

---

[2] Chapter 2 provides more detail on my relevant experience and expertise.

[3] PETER SWIRE & KENESA AHMAD, U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS, INT'L ASSOC. OF PRIV. PROF. (2012) https://iapp.org/media/pdf/certification/cippus-us-private-sector-ch3.pdf.

[4] 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.

[5] 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. 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."

global "benchmark" for transparent principles, procedures, and oversight for national security surveillance.[6]

PART 2:
Systemic Safeguards in US Law and Practice

[14] 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 1970's, 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,[7] and by additional safeguards put in place since then. Overall, many of the most effective protections for privacy, in my view, exist at the *systemic* level, rather than occurring primarily on a retroactive basis through an individual remedy.[8]

[15] This proceeding assesses the adequacy of the protections against excessive surveillance that occur when personal data that is in the EU is transferred to the US. When the US government conducts a wiretap or otherwise gains access to personal data in the US, the investigation within the US is governed primarily by either foreign intelligence or criminal rules.[9]

[16] 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*."[10] For data transfers, the US logically could collect the information in two

---

[6] Brown et al., *supra* note 1.

[7] Swire, *US Surveillance Law*, *supra* note 5.

[8] *See* Swire, *The System of Foreign Intelligence Surveillance Law*, *supra* note 4. The biographical Chapter 2 includes an Annex showing the large number of reforms proposed in the 2004 article that have since become law and practice in the US.

[9] When these searches occur under a mandatory order, they generally 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.

[10] *See* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY 70 (Dec. 12, 2014) [hereinafter "REVIEW GROUP REPORT"], https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (emphasis in original); *see also*

ways. First, if the personal data is collected within the US, then collection is done generally either under law enforcement authorities or foreign intelligence authorities, notably FISA. Second, the US government could seek to gain access to the data while it is being transferred, such as through undersea cables. As discussed in Chapter 3, the EU Commission considered this possibility in its opinion on Privacy Shield, and found adequate protection.[11] In addition, in recent years strong encryption has become standard for transmission of social network, webmail, and other types of communications, so any hypothetical access to undersea cables by an intelligence agency would be difficult or impossible compared to access to unencrypted communications.[12]

I. Systemic Safeguards in Foreign Intelligence

[17] My Testimony summarizes the detailed discussion in Chapter 3 of the systemic safeguards in foreign intelligence. Part A 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. Part B describes the systemic statutory safeguards governing foreign intelligence surveillance. Part C describes the oversight mechanisms, and Part D the transparency mechanisms. Part E describes administrative safeguards that are significant in practice and supplement the legislative safeguards. My Testimony also summarizes how these safeguards apply in a case study, set forth in Chapter 5, on how the Foreign Intelligence Surveillance Court has supplied these safeguards in practice.

[18] 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 privacy expert and Oxford Professor, 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."[13] 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 EU Member States. In addition, the case study on the Foreign Intelligence Surveillance Court 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.

A. The US as a Constitutional Democracy under the Rule of Law

---

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CIVIL LIBERTIES AND PRIVACY OFFICE, CIVIL LIBERTIES AND PRIVACY INFORMATION PAPER: DESCRIPTION OF CIVIL LIBERTIES AND PRIVACY PROTECTIONS INCORPORATED IN THE 2008 REVISION OF EXECUTIVE ORDER 12333 3 (2008, and revised in 2013) https://www.dni.gov/files/documents/CLPO/CLPO_Information_Paper_on_2008_Revision_to_EO_12333.pdf ("FISA information is subject to the provisions of FISA and cannot be affected by Executive Order.").

[11] *See* Chapter 3, Section VI(B).

[12] *See* Peter Swire, Testimony before the US Senate Commerce Comm. on "How Will the FCC's Proposed Privacy Rules Affect Consumers and Competition?" (July 12, 2016) (discussing increasing prevalence of encryption), https://iisp.gatech.edu/sites/default/files/images/swire_commerce_fcc_privacy_comments_07_12_2016.pdf.

[13] Brown et al., *supra* note 1, at 3.

[19] The most fundamental assessment of "adequacy" or "essential equivalence" goes to whether the nation protects rights and freedoms under the rule of law. The US Constitution created a time-tested system of checks and balances among the three branches of government, in continuous operation since 1790. The judiciary is a separate branch of the US government, staffed by independent judges who exercise the power of judicial review.[14] The US Constitution enumerates fundamental rights, which serve as a systemic check against abuse because judges can and do strike down government action as unconstitutional where appropriate.[15]

[20] For protection against government access to personal data, the Fourth Amendment to the US Constitution – which prohibits unreasonable searches of people's "person, houses, papers, and effects" – plays a particularly important role.[16] Foreign intelligence searches on a US person, or on a non-US person who is in the US, remain subject to the Fourth Amendment, because such searches must meet the overall Fourth Amendment test that they be "reasonable."[17] These constitutional protections apply to searches conducted in the US (including on data transferred to the US).[18] As discussed below, the judiciary plays a key role in overseeing surveillance conducted in the US and holding it to constitutional standards.

B. Statutory Safeguards over Foreign Intelligence Surveillance

[21] In addition to constitutional checks, major safeguards in the US system of foreign intelligence law are codified in a number of statutes. The democratically-elected branches in the US have authorized surveillance to protect national security. They also have responded to evidence of excessive surveillance with laws setting limits on surveillance powers.[19]

[22] Most notably, in 1978, the US Congress passed the Foreign Intelligence Surveillance Act (FISA).[20] The first major changes to FISA took place in the USA PATRIOT Act, following the attacks of September 11, 2001. Along with many others, I argued that those changes swept too

---

[14] In regards to guarantees of judges' independence, see Chapter 3, Section I(B). The judicial branch has had the authority to engage in judicial review since the 1803 Supreme Court case of *Marbury v. Madison*, 5 U.S. 137 (1803).

[15] *See* Chapter 3, Section I(C).

[16] *See* U.S. CONST. amend. IV, discussed in further detail in Chapter 3, Section I(C).

[17] *In re Sealed Case*, 310 F.3d 717 (F.I.S.C.R. 2002), http://law.justia.com/cases/federal/appellate-courts/F3/310/717/495663/. For further discussion of the Fourth Amendment in the surveillance context, *see* Chapter 3, Section II(A).

[18] In some European writing about US law, there has been confusion about the effect of US Supreme Court cases defining the scope of the protection offered by the Fourth Amendment, such as *United States v. Verdugo-Urquidez*, 494 U.S. 1092 (1990). [The Fourth Amendment applies to searches within the US, where the non-citizen has "substantial voluntary connections" to the US, such as physical presence in the country. The Supreme Court has not addressed whether the Fourth Amendment would apply to searches of non-citizens' data where the data is located within the US but there has been no "substantial voluntary connection" to the US.] [Note to reader: The discussion of *Verdugo* in this footnote is one of exactly two places where Swire supplemented or modified the original testimony based on review of the testimony of the other experts in the case. The other place is footnote 72 of this chapter.]

[19] Chapter 3, Section II traces the historical events that led to important statutes in place today, including the civil rights movement, investigations following the Watergate affair, the September 11, 2001 attacks, and the Snowden disclosures.

[20] *See* 50 U.S.C. § 1801 *et seq.*, discussed at length throughout Chapter 3.

broadly.[21] There have been numerous pro-privacy reforms since 2001. For instance, following the Snowden disclosures, Congress in the USA FREEDOM Act of 2015 strengthened important aspects of FISA, and ended bulk collection under Section 215 of the PATRIOT Act.[22]

[23] Under FISA and Supreme Court law, judges retain their power to oversee all electronic surveillance conducted within the United States. A search is either (a) conducted in the criminal context, in which case a judge must approve a warrant showing probable cause of a crime; or (b) conducted in the foreign intelligence context, in which case the Foreign Intelligence Surveillance Court must authorize the surveillance pursuant to FISA and subject to the reasonableness requirements of the Fourth Amendment. These are the principle ways that an electronic communications search is carried out lawfully within the US.[23]

[24] This section addresses three systemic statutory safeguards the US has placed over foreign intelligence: (1) the Foreign Intelligence Surveillance Court; (2) metadata collection under Section 215; and (3) communications collection under Section 702.

1. The Foreign Intelligence Surveillance Court

[25] Since passage of FISA, the Foreign Intelligence Surveillance Court (FISC) has played a central role in regulating US foreign intelligence. FISA grants the FISC exclusive jurisdiction to issue orders for all foreign-intelligence surveillance carried out in the US.[24] These include orders for individual surveillance, as well as oversight of larger intelligence programs.

[26] Within the FISC, independent and high-quality judges with lifetime appointments to the federal bench gain access to top-secret information, and exercise constitutional authority in enforcing legal limits on intelligence activities.[25] FISC judges are selected for service by the Chief Justice of the US Supreme Court, and supported by a staff of security-cleared attorneys with expertise in national security law.[26]

---

[21] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. 107-56 (2001). I discuss the PATRIOT Act in Chapter 3, Sections II(C) and III(B), and a set of ten reforms in the Annex to Chapter 2.

[22] *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. No. 114-23 (2015). Reforms introduced by the USA FREEDOM Act are discussed throughout Chapters 3 and 5.

[23] 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 (ECPA) of 1986 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 4.

[24] *See* 50 U.S.C. § 1804(a).

[25] Federal judges are appointed to the Foreign Intelligence Surveillance Court for seven year terms. For extensive discussion of the FISC's institutional structure and its resources for overseeing US foreign intelligence, *see* Chapter 3, Section III(A)(1).

[26] *See id.*

[27] Recently, the FISC and the Obama Administrative declassified numerous FISC pleadings, orders, and related materials. To determine how the FISC has applied in practice the safeguards identified in this Testimony, I devote Chapter 5 to a detailed review of the declassified materials. I find the materials support the following conclusions:

The FISC today provides independent and effective oversight over US government surveillance, backed by thorough review proceedings and constitutional judicial authority.[27] The FISC's standard procedures subject government surveillance applications to careful review, and FISC decisions show the court requiring the government to withstand rounds of briefing, meetings, questions, and hearings. In its evaluations of proposed surveillance, the FISC focuses on government compliance with existing or similar prior FISC orders. In recent years, the number of surveillance applications the FISC modified or rejected has grown substantially, and the FISC has exercised its constitutional power to halt surveillance it determines is unlawful.

The FISC monitors compliance with its orders, and has enforced with significant sanctions in cases of noncompliance.[28] The FISC's jurisdiction extends to monitoring and enforcing its orders. A system of reporting rules, third-party audits of surveillance agencies, and periodic reporting provide the FISC with notice of compliance incidents. When the FISC encounters noncompliance, it has imposed significant sanctions, at times denying the NSA access to intelligence data and threatening to terminate entire surveillance programs unless changes are implemented.

In recent years, the FISC on its own initiative as well as new legislation have greatly increased transparency.[29] FISC proceedings are secret and, traditionally, FISC decisions have been classified. However, in recent years, the FISC itself began to release more of its own opinions and procedures, and the USA FREEDOM Act now requires significant FISC decisions to be published. In addition, FISC litigation resulted in corporate transparency reporting rights that the USA FREEDOM Act subsequently codified and expanded.

The FISC now receives and will continue to benefit from adversarial briefing by non-governmental parties in important cases.[30] During the post-2001 period, the FISC's role expanded from approving individual wiretap orders to overseeing entire foreign intelligence programs, and there was increasing recognition that the FISC would benefit from adversarial presentation of complex issues. In some cases, the FISC began to receive such briefing of its own initiative, including both from privacy experts and communications service providers. Now, the USA FREEDOM Act has created a panel of six privacy experts who will have access to classified information and will participate via briefing and oral argument in important FISC proceedings.

---

[27] The materials underlying this conclusion are discussed in detail in Chapter 5, Section I.
[28] *See id.*, Section II.
[29] *See id.*, Section III.
[30] *See id.*, Section IV.

2. Collection of Metadata under Section 215

[28] Perhaps the most dramatic change in US surveillance statutes since 2013 concerns reforms of Section 215 of the USA PATRIOT Act, which provided the government with broad powers to obtain "documents and other tangible things."[31] After the September 11 attacks, Section 215 was used as a basis for collecting metadata on large numbers of phone calls made in the US.[32]

[29] The USA FREEDOM Act abolished bulk collection under Section 215 and two other similar statutory authorities. These limits on collection apply to both US and non-US persons. A far narrower authority now exists, based on individualized selectors associated with terrorism and judicial review of each proposed selector.[33]

3. Collection of Communications under Section 702

[30] Section 702 of FISA applies to collections that take place within the US, and only authorizes access to the communications of targeted individuals, for listed foreign intelligence purposes.[34] The independent Privacy and Civil Liberties Oversight Board, after receiving classified briefings on Section 702, came to this conclusion:

> 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.[35]

[31] Chapter 3 on systemic safeguards for foreign intelligence and Chapter 5 on the FISC provide detail about the PRISM and Upstream programs under Section 702. Misunderstanding about the PRISM program traces to the original and since-revised Washington Post story, which stated that "[t]he National Security Agency and the FBI are tapping *directly* into the central servers of nine leading U.S. Internet companies" to extract a range of information.[36] This statement was incorrect. In practice, PRISM operates under a judicially-approved and judicially-

---

[31] *See* USA PATRIOT Act § 215. Concerns about and reforms to Section 215 of the PATRIOT Act are discussed detail in Chapter 3, Section III(B).

[32] Chapter 3, Section III(B) discusses the post-September-11 collection of metadata under Section 215.

[33] These reforms are codified at 50 U.S.C. § 1861 and explained in further detail in Chapter 3, Section III(B).

[34] Section 702 is codified at 50 U.S.C. § 1881a. A detailed discussion of the history, structure, and operations of Section 702 is contained in Chapter 3, Section III(B).

[35] PRIVACY & 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.

[36] *See* Barton Gellman, *U.S. intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST (Jun. 6, 2013) (emphasis added), https://www.engadget.com/2013/06/06/washington-post-nsa-fbi-tapping-directly-into-servers-of-9-lea/. The story was revised to explain that a leaked document said that there was direct access; in fact, as explained in Chapter 3, Section III(C)(2), the leaked document was misleading or incorrect; Section 702 does not authorize direct access.

supervised directive, pursuant to which the government sends a request to a US-based provider for collection of targeted "selectors," such as an email address.

[32] There have also been concerns about Upstream as a mass collection program.[37] In fact, the US government receives communications under both Upstream and PRISM based on targeted selectors, with actions under each program subject to FISC review. Concerning scale, a declassified FISC opinion found that over 90% of the Internet communications obtained by the NSA in 2011 under Section 702 actually resulted from PRISM, with less than 10% coming from Upstream.[38] The US intelligence community now releases an annual Statistical Transparency Report,[39] with the statistics subject to oversight from Congress, Inspector Generals, the FISC, the Privacy and Civil Liberties Oversight Board, and others.[40] 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.[41] That is a tiny fraction of US, European, or global Internet users. Rather than having mass or unrestrained surveillance, the documented statistics show the low likelihood of communications being acquired for ordinary citizens.[42]

[33] I have testified previously that Section 702, in my view, is a reasonable response to changing technology, set forth in a statute that was debated publicly prior to its enactment.[43] The now-declassified FISC materials, along with reports on Section 702 by the Privacy and Civil Liberties Oversight Board and the Review Group, show a far more targeted and legally-constrained set of actions under Section 702 than press accounts had initially suggested.[44]

C. Oversight of Surveillance Activities

---

[37] Chapter 3, Section III(C)(3) contains a more detailed description of Upstream collection.
[38] *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.
[39] Transparency reports have been released for every year since 2013: 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; 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; 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.
[40] For a listing of the multiple oversight entities, *see* REVIEW GROUP REPORT, *supra* note 10, Appendix C at 269.
[41] The statistical reports define "target" in detail, and my assessment is that the number of individuals targeted is lower than the reported number.
[42] 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." *See, e.g.*, 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.
[43] *See* Swire, *US Surveillance Law*, *supra* note 5.
[44] *See* Chapter 3, Section III(C)(1).

[34] In addition to codifying systemic safeguards, the US has established multiple review and oversight mechanisms related to foreign intelligence. Following the Snowden disclosures, I was one of five members of the Review Group on Intelligence and Communications Technology that President Obama created to conduct a comprehensive review of US surveillance programs. We received top-secret briefings and presented our report of over 300 pages to the President in December 2013.[45] In January 2014, the Obama Administration informed us that 70 percent of our 46 recommendations had been adopted in letter or spirit, and others have been adopted since that time.

[35] Going forward, multiple institutions, each with access to classified information, exercise oversight responsibilities over foreign intelligence activities:[46]

1. *Executive Agency Inspectors General (IGs)*. By statute, IG offices are established within US agencies to independently police the legality of agency activity, and to receive reports of illegal activity from government employees.[47] Every intelligence agency, including the NSA, has an IG office.

2. *Congressional Oversight Committees*. Both the US Senate and House of Representatives have Intelligence oversight committees, with subpoena power and access to classified information.[48] Whistleblower laws provide that government employees and contractors can report serious problems related to surveillance directly to both committees.[49]

3. *Privacy and Civil Liberties Oversight Board ("PCLOB")*. The PCLOB is an independent privacy agency with substantial investigative powers over classified foreign intelligence activities.[50] PCLOB-issued reports have resulted in significant changes to US surveillance practice.[51]

4. *Privacy Offices in Executive Agencies.* President Obama recently issued an executive order founding the Federal Privacy Council, which is responsible for implementing privacy policy throughout US government agencies.[52] US intelligence agencies now have internal offices devoted to privacy and civil

[45] REVIEW GROUP REPORT, *supra* note 10, at 179.
[46] For a more discussion of each listed oversight body, see Chapter 3, Section IV.
[47] *See generally* Inspector General Act of 1978, codified at 5 U.S.C. App. 1 §§ 1-13.
[48] *See generally U.S. Senate Select Committee on Intelligence*, Senate.gov, http://www.intelligence.senate.gov/. For a more detailed discussion of Congressional oversight committees, *see* Chapter 3, Section IV(B).
[49] *See* Intelligence Community Whistleblower Protection Act of 1998, 50 U.S.C. § 403q. Chapter 3, Section IV(B) discusses the procedures for reporting violations to the Congressional committees.
[50] *See* 42 U.S.C. § 2000ee. PCLOB's purpose, structure, and powers are discussed in detail in Chapter 3, Section IV(C).
[51] To date, PCLOB has issued two reports on Section 215 collection and Section 702 programs. Both reports, including changes as a result of PCLOB's recommendations, are discussed in Chapter 3, Section IV(C).
[52] *See* 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.

liberties.[53] The Department of Justice's National Security Division Office of Intelligence has established an Oversight Section.[54] An extensive oversight system also exists to report compliance incidents to the Foreign Intelligence Surveillance Court.[55]

D. Transparency Safeguards

[36] The US system of foreign intelligence surveillance law has long had important transparency requirements, such as statistical reports about the number of court orders issued. Since 2013, there have been numerous changes in the direction of transparency, while recognizing the harm to national security that can result from disclosure of classified information, such as about the sources and methods of intelligence activity. The transparency safeguards complement oversight by the FISC and the other oversight mechanisms just discussed – transparency is appropriate where possible consistent with national security, and additional oversight is performed by judges and others with top-secret clearances where transparency is not appropriate.

[37] As discussed in greater detail in the following chapters,[56] transparency safeguards in the US include:

1. *Reports on legal interpretations.* The USA FREEDOM Act included a new rule addressing the risk of secret law. When the FISC issues a decision that contains "a significant construction or interpretation of any provision of law," the USA FREEDOM Act now requires the US government to make the FISC decision publicly available to the greatest practicable extent.[57]

2. *Government transparency reports.* The USA FREEDOM Act provided for considerably greater detail than before about government requests for foreign intelligence information, including the annual US Statistical Transparency Report.[58]

---

[53] Chapter 3, Section IV(D) discusses privacy offices within the US intelligence community, such as the NSA's Civil Liberties and Privacy Officer.
[54] DEP'T OF JUSTICE, *Office of Intelligence* (July 23, 2014), https://www.justice.gov/nsd/office-intelligence.
[55] Chapter 5, Section II(A).
[56] Chapter 3, Section IV and Chapter 5, Section III.
[57] 50 U.S.C. § 1872(b), https://casetext.com/statute/50-usc-1872-declassification-of-significant-decisions-orders-and-opinions. If the opinion cannot be declassified for national security reasons, then the government must still publish an unclassified summary.
[58] Transparency reports have been released for every year since 2013:
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; 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; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics*

3. *Company transparency reports.* The USA FREEDOM Act codified and expanded the ability of companies to provide granular information in their transparency reports about the orders to which they replied.[59] Companies for instance now can report the range of FISA orders for content and non-content (e.g., 0-1,000; 1,001-2,000), as well as the number of customer selectors targeted under those orders. Relevant to the claims of mass and indiscriminate surveillance, those reports show the very small fraction of users who have been subject of Section 702 and other requests to the companies.[60]

4. *Additional government transparency actions.* Going beyond statutory requirements, the US government since 2013 has taken multiple transparency actions, including: declassification of numerous FISC decisions;[61] a new website devoted to public access to intelligence community information;[62] the first "Principles of Intelligence Transparency for the Intelligence Community";[63] and posting of agencies' policies under intelligence authorities including Executive Order 12,333.[64]

E. Executive Safeguards

[38] Since 2013, the US Executive Branch has instituted multiple safeguards to supplement the legislative protections outlined above. My experience in the Review Group and more generally leads to my conclusion, detailed in Section VI(A) of Chapter 3, that these Executive Branch safeguards matter a great deal in practice.

[39] Foremost among the new executive-branch safeguards is Presidential Policy Directive 28 (PPD-28), which mandates that US surveillance agencies make privacy integral to signals intelligence planning.[65] PPD-28 requires that agencies prioritize alternative sources of information – such as diplomatic sources – over signals intelligence.[66] Where surveillance is

---

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

[59] Chapter 3, Section V(E).

[60] Chapter 3, Section V(E) reviews the most recent Facebook and Google transparency reports and finds that, at most, approximately .001% of Google users are potentially affected by US information requests.

[61] *See* U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Public Filings*, http://www.fisc.uscourts.gov/public-filings; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Declassified: Release of FISC Question of Law and FISCR Opinion*, IC ON THE RECORD (Aug. 22, 2016), https://icontherecord.tumblr.com/tagged/declassified.

[62] *See* IC ON THE RECORD, https://icontherecord.tumblr.com/.

[63] *See* 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.

[64] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *IC on the Record Statement Accompanying Posting of EO 12333 Table of Guidelines*, IC ON THE RECORD (July 20, 2016), https://icontherecord.tumblr.com/post/147708188298/ic-on-the-record-statement-accompanying-posting-of.

[65] Chapter 3, Section VI(B) contains a detailed discussion of six significant safeguards contained in PPD-28. *See Presidential Policy Directive 28, Signals Intelligence Activities* (PPD-28) (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[66] *See* PPD-28, § 1(d).

used, it must be "as tailored as feasible," proceeding via selectors such as email addresses whenever practicable.[67] Bulk collection cannot be used except to detect and counter serious threats, such as terrorism, espionage, or nuclear proliferation.[68] Data about EU citizens cannot be disseminated unless the same could be done with comparable data about US persons.[69] Although PPD-28 does not use terms from EU law such as "necessary" and "proportionate," prioritizing alternatives to surveillance and requiring tailored collection and use limits are examples of US law implementing specific safeguards to address these concerns.

[40] Additionally, recent agreements between the EU and US bind the US executive branch to safeguard EU citizens' personal data. The EU-US Umbrella Agreement protects personal data transferred to US agencies for law-enforcement purposes, restricting transfers and permissible uses, and providing EU residents with access and correction rights.[70] The Privacy Shield contains commitments from the US government to act promptly and effectively to address EU data protection concerns – and subjects Privacy Shield performance to an annual review process.[71] These commitments and reviews provide the EU and its DPAs an ongoing mechanism to protect personal data transferred to the US, including data processed for national security purposes.

II. Systemic Safeguards in Law Enforcement

[41] In addition to foreign intelligence, the US has established a system of safeguards protecting individuals in the context of criminal investigations. As mentioned above, government collection of electronic communications in the US takes place primarily either under law enforcement or foreign intelligence legal authorities. For collection in the US, any other authority such as Executive Order 12,333 does not apply.[72] This part of my Testimony outlines the systemic safeguards in place for collection in the US of electronic communications in criminal investigations.

---

[67] *See id.*
[68] *See id.* § 2.
[69] *See id.* § 4(a)(i).
[70] *See* Agreement between the European Union and the United States of America on the Protection of Personal Data When Transferred and Processed for the Purpose of Preventing, Investigating, Detecting or Prosecuting Criminal Offences (Draft for Initialing), EU-US, June 2, 2016, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf [hereinafter "Umbrella Agreement"].
[71] *See The EU-U.S. Privacy Shield*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.
[72] To be explicit, my assumption in writing this Testimony is that the Court is considering the adequacy of protection for data that is transferred to the US, and not for data that remains in the EU. Based on that assumption, I focus my analysis on the legal rules that apply to data transfers. By contrast, Executive Order 12,333 applies to data collected outside of the US. [There is a "transit authority" exception to the application of Executive Order 12,333. My understanding is that transit authority would apply, for instance, to an email that went from a foreign origin, across the telecommunications network within the U.S. without having a U.S. destination, and then went to a foreign destination. For a discussion of transit authority, see https://www.lawfareblog.com/understanding-deeper-history-fisa-and-702-charlie-savages-power-wars-fiber-optic-cables-and- transit.] [Note to reader: The discussion of transit authority in this footnote is one of exactly two places where Swire supplemented or modified the original testimony based on review of the testimony of the other experts in the case. The other place is footnote 18 of this chapter.]

[42] Reacting to the US colonial experience with English monarchs, the US Constitution sets forth multiple fundamental rights to check government overreach in criminal cases.[73] These rights have resulted in multiple areas where the US is stricter than other countries, including many EU countries, in providing criminal procedure safeguards:

1. *Strict Judicial Oversight*.[74] Independent judicial officers oversee applications for warrants to conduct searches and collect evidence. "Probable cause," the requirement for granting a warrant to search, is a relatively strict requirement for digital searches.[75]

2. *Stricter Oversight for Interceptions*. Telephone wiretaps and other real-time interception have even stricter requirements, such as successive rounds of agency review, minimization safeguards for non-targets, and requirements to exhaust other sources of information.[76]

3. *Penalties for Illegal Searches*. The so-called "exclusionary rule" bars evidence obtained through an illegal search from being used at criminal trials,[77] while the "fruit of the poisonous tree" doctrine further bars additional evidence derived from the illegal search.[78] Officers who conduct illegal searches are subject to civil damages lawsuits.[79]

4. *Orders Permit Legal Challenges*. US law requires court orders to clearly indicate the legal basis for a warrant or information request, permitting the recipient to determine whether there is a basis to challenge the order.[80]

5. *No Mandatory Data Retention*. US law does not require data retention for Internet communications, such as email.[81] For telephone communications, US law requires limited retention of records needed to resolve billing disputes.[82]

6. *Strong Encryption*. The US permits the use of strong encryption, a privacy-preserving technology, which has been widely adopted by US-based technology companies.[83]

---

[73] Chapter 4, Section I discusses various rights enshrined in the Bill of Rights to the US Constitution as a response to the US colonial experience with England.
[74] Chapter 4, Sections II(A), II(B), and II(E) provide a detailed discussion of judicial oversight and probable cause.
[75] *See, e.g.*, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), https://scholar.google.com/scholar_case?case=11707608375476732 55&hl=en&as_sdt=6&as_vis=1&oi=scholarr.
[76] *See* 18 U.S.C. § 2518, discussed in Chapter 4, Section II(C).
[77] *See Mapp v. Ohio*, 367 U.S. 643 (1961). The exclusionary rule and other penalties for illegal searches are discussed in Chapter 4, Section II(D).
[78] *See Wong Sun v. U.S.*, 371 U.S. 471 (1963).
[79] *See* 42 U.S.C. §1983; *Bivens v. Six Unknown Agents*, 403 U.S. 388 (1971).
[80] *See* 18 U.S.C. § 2703(b).
[81] For a more comparison of EU data retention practice and limited US data retention rules, *see* Chapter 4, Section II(G).
[82] *See* 47 C.F.R. § 42.6.

[43] In significant measure, the creation of the United States itself derived from an insistence on protecting the rights of individuals in the criminal justice system. Although it is a complex task to assess precisely where the US and EU provide stricter safeguards in criminal investigations, the US has significant, and often constitutional, safeguards that often are lacking in the EU. In my view, a fair comparison of the adequacy of the two systems should carefully consider such additional factors.

III. Conclusion on Systemic Safeguards

[44] 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 ensure oversight by persons with access to classified information for the necessarily secret activities, and to create transparency in ways that do not compromise national security. In my view, the US system provides effective checks against abuse of secret surveillance powers. I agree with the team led by Oxford Professor Ian Brown, who after comparing US safeguards to other countries, concluded that "the US now serves as a baseline for foreign intelligence standards," and that 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."[84] In addition, as shown in the detailed study of the Foreign Intelligence Surveillance Court, those rigorous legal standards are effectively implemented in practice, under the supervision of independent judges with access to top-secret information.

PART 3: Individual Remedies in US Privacy Law

[45] In the US, an EU resident or other individual has multiple remedies available for violations of privacy. These individual remedies work in tandem with the systemic safeguards just discussed. For many issues involving secret surveillance by agencies, I believe systemic safeguards are often particularly effective. In the US, oversight bodies such as the FISC, the PCLOB, agency Inspectors General, the Senate and House Intelligence Committees, and the President's Review Group that I served on gain access to classified information. That access allows these overseers to detect privacy problems and take action to correct them. By contrast, there are reasons to be cautious about disclosing national security secrets to individuals or in open court, where the act of disclosure itself can pose new security risks.

[46] The US system bolsters those systemic safeguards with a multi-pronged approach to individual remedies. I have sometimes encountered the view in the EU and elsewhere that the US lacks remedies generally for privacy violations, or that remedies are only available to US persons. That is not correct. As the lead author of the textbook for the International Association of Privacy Professionals (IAPP) US private-sector privacy law exam, I wrote an overview of US

---

[83] *See* Chapter 4, Section II(H); *see also* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416 (2012).
[84] Brown et al., *supra* note 1, at 3.

privacy laws that apply to the private sector, including enforcement mechanisms, that on its own took nearly 200 pages and eleven chapters.[85] Annex 1 to Chapter 7 of my Testimony also charts this combination of systemic safeguards and individual remedies to provide an overview of the US legal privacy regime in total, as complement to the detailed explanations provided of each aspect of that regime in Chapters 3, 4, and 7.

[47] The large quantity of US privacy laws sometimes leads to a different critique from the EU, that US remedies are "fragmented" and may for that reason may not be adequate under EU standards. I hope that this explanation of US privacy remedies can demonstrate how the different pieces of US law fit together. The complexity of US law arises in part from its pro-enforcement legal culture, with the result that multiple privacy enforcers each may have the legal ability to bring an action. This division of authority can be beneficial for privacy protection, as it allows subject matter experts to enforce in their areas of expertise, allows multiple agencies to leverage their resources to police categories of activity on behalf of data subjects, and also allows private rights of action for individuals.

[48] To explain the US privacy enforcement system, I outline here the paths an aggrieved person in the US or EU may take in response to concerns regarding US privacy violations, as explained more fully in Chapter 7: Individual Remedies in US Privacy Law. First, I discuss individual judicial remedies against the US government, including the recently-finalized Privacy Shield and Umbrella Agreement, as well as the recently passed Judicial Redress Act. Next, I examine the civil and criminal remedies available where individuals, including government employees, violate wiretap and other surveillance rules under laws such as the Stored Communications Act, the Wiretap Act, and the Foreign Intelligence Surveillance Act. After that, I highlight three paths of non-judicial remedies individuals can take: the PCLOB, Congressional committees, and recourse to the US free press and privacy-protective non-governmental organizations. Next, I talk about individual remedies against US companies that improperly disclose information to the US government about customers. These causes of action against US companies can be brought both by individuals (US and non-US) as well as by US federal administrative agencies. I also examine remedies available under state law in the US and private rights of action, including enforcement by state Attorneys General.

[49] I also provide in this part an answer to some of the concerns raised in the Irish Data Protection Commissioner's Affidavit in this case. Specifically, I respond to the Affidavit's concerns regarding fragmented remedies in US law, possible limitations on the availability of remedies, and concerns regarding the doctrine of standing under US law. This part explains how the overall US legal system addresses these concerns, and how specific reforms such as the Ombudsman mechanism in the Privacy Shield Framework affect these concerns.

---

[85] PETER SWIRE & KENESA AHMAD, U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS, INT'L ASSOC. OF PRIV. PROF. (2012) https://iapp.org/media/pdf/certification/cippus-us-private-sector-ch3.pdf. The same year, we published a book providing an introduction to privacy globally. PETER SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS, AND PRACTICES, INT'L ASSOC. OF PRIV. PROF. (2012).

[50] Part 3 concludes with a caveat – individual remedies are sometimes difficult to provide in the intelligence setting, because of the risk of revealing classified information to hostile actors. The desirability of individual remedies, in intelligence systems, thus depends on the advantages of providing an individual remedy against the risks that come from disclosing classified information. Put in the language of Article 8 of the European Convention of Human Rights, the desirability of individual remedies, in intelligence systems, depends on how implementation of the right is judged with the necessity in a democratic society of protecting other interests including national security and public safety.

I. Individual Remedies Against the United States Government

[51] Remedies exist against the US government for privacy violations under both civil and criminal statutes.

A. US Civil Judicial Remedies

[52] Qualifying individuals, including EU persons, may bring civil suits against the US government for violations of law that can result in monetary damages and injunctions against ongoing illegal government programs or activities. Remedies of this sort exist under: the Judicial Redress Act; the EU-US Privacy Shield; the Umbrella Agreement; the Stored Communications Act (SCA); the Wiretap Act; and the Foreign Intelligence Surveillance Act (FISA).

[53] Taken together, the EU-US Privacy Shield, the Judicial Redress Act, and the Umbrella Agreement provide important individual legal remedies for EU persons who believe they have suffered privacy harms.[86] The EU-US Privacy Shield created new remedies against the US government available to EU persons. The Privacy Shield creates an Ombudsman within the US Department of State who can hear complaints from EU data subjects related to US government actions.[87] This Ombudsman operates independently from US national security services, and the protections apply to data transfers under Standard Contractual Clauses: the Ombudsman has the authority to review "requests relating to national security access to data transmitted from the EU to the US pursuant to the Privacy Shield, standard contractual clauses [and] binding corporate rules (BCRs)."[88] The Privacy Shield also allows individuals to invoke, free of charge, an

[86] For a more detailed discussion of these documents, including the criteria for qualifying individuals under the Act, *see* Chapter 7, Section I(A)(1).

[87] European Commission Press Release MEMO16/434, *EU-U.S. Privacy Shield: Frequently Asked Questions*, (Feb. 29, 2016), http://europa.eu/rapid/press-release_MEMO-16-434_en.htm. Note that, as of today, this mechanism is still being organized and is not yet available. *See* PRIVACY SHIELD FRAMEWORK, *How to Submit a Request Relating to U.S. National Security Access to Data*, https://www.privacyshield.gov/article?id=How-to-Submit-a-Request-Relating-to-U-S-National-Security-Access-to-Data.

[88] European Commission, Annexes to the Commission Implementing Decision 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, C(2016) 4176 final (July 12, 2016) at 52, http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf, [hereinafter Annexes]. Note that the Ombudsman can also review requests submitted in response to data transmitted from the EU to the US under derogations and possible future derogations.

independent alternative dispute resolution body to handle complaints against US companies participating in the Privacy Shield.[89]

[54] Under the Judicial Redress Act of 2016,[90] the US expressly extended the right to a civil action against a US governmental agency to obtain remedies with respect to the willful or intentional disclosure of covered records in violation of the Privacy Act or when a designated US governmental agency or component declines to amend an individual's record in response to an individual request.[91] The Judicial Redress Act directly addresses a concern that had previously been expressed by EU officials: that EU citizens were not afforded protections under the Privacy Act. Although EU Member States have not to date finalized their participation under the Judicial Redress Act, my understanding is that the EU and US plan to do so.

[55] The Privacy Act allows US and qualifying non-US persons to sue a US federal agency for the improper handling of covered records; to obtain injunctions or monetary damages; and to review, copy, and request amendments to their records.[92] An individual may sue under the Act when the agency willfully or intentionally fails to comply with the Privacy Act in a way that has "an adverse impact on [the] individual."[93] An individual also qualifies to sue if an agency determines not to amend the individual's record in response to a request, fails to provide appropriate review based on a request, or refuses to comply with a request.[94] As discussed further in Chapter 7, there are exceptions to the applicability of the Privacy Act.

[56] The Umbrella Agreement provides remedies for EU data subjects whose data is transferred to US law enforcement authorities. Individuals can access this personal information, subject to certain restrictions equivalent to what US citizens face, and EU data subjects may request correction or rectification.[95] If a law enforcement agency denies an access or rectification request, it must explain its basis for denial "without undue delay." The EU data subject may, in accordance with the applicable US legal framework, seek administrative and judicial review of such denial, or seek judicial review of any alleged willful or intentional unlawful disclosures of the personal information.[96] If appropriate, the court may require access or rectification, and with respect to other violations, may award compensatory damages.[97] These

---

[89] *Annexes*, *supra* note 88 at 19, http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf; European Commission Directorate General for Justice and Consumers, *Guide to the EU-U.S. Privacy Shield* (2016), http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf.
[90] 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.
[91] *Id.* at § 2(a).
[92] 5 U.S.C. § 552a(g)(1); *see also id.* at § 2(h)(4) (defining "covered record" as the same as a record under 5 U.S.C. § 552a(a)(4)).
[93] *Id.*
[94] *Id.*
[95] *See* Proposal for a Council Decision on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, at 10-12, COM (2016) 237 final (Apr. 29, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476055815798&uri=CELEX:52016PC0237.
[96] *Id.*
[97] *Id.*

abilities are granted in part by the Judicial Redress Act, passage of which was due in part to a requirement of the Umbrella Agreement.[98]

[57] The Stored Communications Act provides a remedy for both US and EU citizens for unlawful access to or use of stored communications data by an unauthorized individual government actor or US agency.[99] The rules for lawfully accessing stored data turn on the type of data. For the content of communications, such as email, an independent judge applies the Fourth Amendment's constitutional rule, requiring probable cause of a crime.[100] Access to metadata[101] requires the government to certify to a judge that the information likely to be obtained is relevant to an ongoing criminal investigation.[102] A company can voluntarily disclose basic subscriber information (BSI), and the government can compel access to BSI through other judicial process such as a grand jury subpoena.[103] A data subject whose data is unlawfully accessed can bring suit under the SCA against individual officers and US agencies if the violation was "willful."[104] Successful suits against individual officers can result in money damages of at least $1,000 USD, equitable or declaratory relief, attorney's fees, legal fees, and/or punitive damages.[105] Any government employee found to have willfully or intentionally violated the Act can also be subject to discipline.[106] Suits against a US agency may result in actual damages or $10,000 USD, whichever is greater, plus litigation costs.[107]

[58] The Wiretap Act provides a similar right of action for individuals against the US government.[108] Under the Wiretap Act, the government must show both probable cause and a number of other standards, including a sufficiently serious crime[109] and an explanation of why the information cannot be obtained by other means.[110] Wiretaps are only authorized for a

---

[98] *See Press Release – Questions and Answers on the EU-US data protection "Umbrella Agreement"*, EUROPEAN COMMISSION (Sep. 8, 2015), http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.
[99] For a more detailed discussion of the Stored Communications Act, please see Chapter 7, Section I(A)(2).
[100] The statute itself applies varying standards for access to the content of an email, depending on factors such as whether the email has been opened and how old it is. 18 U.S.C. § 2703. Based on the Fourth Amendment, however, a federal appellate court held in the leading *Warshak* case that individuals have a reasonable expectation of privacy in the contents of an email, and that the relatively strict probable cause standard applies. *U.S. v. Warshak*, 631 F.3d 266, 274 (6th Cir. 2014). The US government has publicly stated that it seeks the content of an email under that probable cause standard. *ECPA (Part 1): Lawful Access to Stored Content: Hearing before the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong., 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Attorney Gen., Office of Legal Policy, Dep't of Justice), https://judiciary.house.gov/_files/hearings/printers/113th/113-16_80065.PDF.
[101] Metadata includes dialing, routing, addressing, and signaling information related to an electronic communication.
[102] 18 U.S.C. §§ 3121-22.
[103] *Id.* §§ 2702-03.
[104] *Id.* § 2520. The civil provision requiring "willful" violation has exceptions for good faith reliance on court orders, grand jury subpoenas, legislative authorizations, statutory authorizations, or a valid request from an investigative or law enforcement officer. 18 U.S.C. § 2520(d). Similarly, there is no "willful" violation where the individual or agency being sued made a good faith determination that the alleged action was valid under ECPA. *Id.*
[105] 18 U.S.C. § 2707(c).
[106] *Id.* § 2707(d).
[107] *Id.* § 2712(a).
[108] For a more detailed discussion of the Wiretap Act, please see Chapter 7, Sections I(A)(2) and III(A)(2).
[109] 18 U.S.C. § 2518(3)(a).
[110] *Id.* § 2518(3)(c).

specific and limited time,[111] must minimize the amount of non-relevant information intercepted,[112] and any surveillance conducted outside those bounds is considered unlawful.[113] Applications under the Wiretap Act must also be approved at the highest levels of the DOJ before they can be submitted to a judge for review. Like the SCA, the Wiretap Act also allows aggrieved individuals, including EU persons, to file suit when their communications have been unlawfully intercepted by the US government.[114] If an individual has "intentionally" violated the Act,[115] a data subject may obtain "appropriate relief,"[116] including an injunction of any ongoing wiretaps, monetary damages, and punitive damages.[117]

[59] FISA also provides individual remedies for data subjects against the unlawful acts of individual government officers.[118] Any surveillance of a data subject performed without statutory or Presidential authorization, misuse of surveillance information, or unlawful disclosure of surveillance information by an individual officer makes that officer liable to suit in US court.[119] Data subjects who successfully sue such officers can receive actual damages greater than or equal to $1,000 USD, statutory damages of $100 USD per day of unlawful surveillance, and potential additional punitive damages and attorney's fees if appropriate.[120] An EU data subject may sue under FISA as long as he or she is not a "foreign power" or an "agent of a foreign power."[121]

B. US Criminal Judicial Remedies

[60] The US Department of Justice can bring criminal charges for violation of the SCA, ECPA, FISA, or the Privacy Act.[122] Careful attention to privacy criminal violations is consistent with the US commitment to effectively enforce violations of privacy law, as demonstrated in the Judicial Redress Act, Umbrella Agreement, and EU-US Privacy Shield Framework.[123] For example, the EU-US Privacy Shield Framework's section on Recourse, Enforcement, and

---

[111] *Id.* § 2518(4)(d).
[112] *Id.* § 2518(5).
[113] *Id.* § 2518(5) ("Every order . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter").
[114] *See* 18 U.S.C. §§ 2510(6), 2510(11) (defining "person" and "aggrieved person" under the statute); *see also Suzlon Energy v. Microsoft*, 671 F.3d 726, 731 (9th Cir. 2011) ("The ECPA protects the domestic communications of non-citizens"). Since The Wiretap Act is codified under ECPA, *Suzlon* likewise applies to available remedies under 18 U.S.C. § 2520.
[115] 18 U.S.C. § 2511(1)(a).
[116] *Id.* § 2520.
[117] *Id.* § 2520(b). Unlike the SCA, the Wiretap Act does not expressly grant a waiver of sovereign immunity for suits against US agencies, but rather allows for suit only against individual officers who have intentionally violated the Act. 18 U.S.C. § 2511(1).
[118] For a more detailed discussion of FISA, please see Chapter 7, Section I(A)(4).
[119] 50 U.S.C. §§ 1801, 1810.
[120] *Id.* § 1810. Note that the individual may receive either actual damages not less than $1,000 USD or $100 USD per day of surveillance, but not both.
[121] *Id.* §§ 1801(a)-1801(b).
[122] For more detailed information about the criminal penalties for such violations, please see Chapter 7, Section I(B).
[123] *See* Umbrella Agreement, *supra* note 70; PRIVACY SHIELD FRAMEWORK, *Recourse, Enforcement and Liability*, https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY; Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2015).

Liability includes a commitment that the FTC will "give priority consideration to referrals of non-compliance with the Principles from the Department and EU Members State authorities."[124]

[61] Additionally, in the event that the US government should attempt to use unlawfully acquired information against a data subject in a criminal proceeding, those data subjects, including EU persons, have two important rights. First, the exclusionary rule allows data subjects to suppress unlawfully obtained evidence from use in court.[125] US courts not only bar the illegally obtained evidence, but also bar evidence acquired as a result of that illegal search or seizure.[126] If such a request is denied at trial, the data subject has the right to appeal that decision.[127]

[62] The Classified Information Procedures Act (CIPA) also provides a mechanism for allowing criminal defendants to access classified materials at trial that may be helpful to the defense.[128] CIPA provides procedures that both protect the security of classified information while allowing criminal defendants to compel the production of evidence related to their defense.[129] In short, CIPA protects both the US government's interest in keeping classified data secret and criminal defendants' right to a fair trial.

II. Non-Judicial Individual Remedies in the US against the US Government

[63] In addition to judicial remedies, there are important administrative, legislative, and public channels for data subjects to seek redress for privacy harms by the US government. Part 2 of this Testimony discussed the systemic safeguards provided by the PCLOB and the Congressional Intelligence committees. The PCLOB and the committees also serve as a way for individuals to submit concerns related to US intelligence practices, for both US and EU persons.

[64] The free press of the US can serve as an important remedy for persons harmed by US surveillance. In contrast to the Official Secrets Acts in other countries, the First Amendment of the US Constitution has been interpreted to strictly protect the freedom of US journalists to report on national security issues such as surveillance. It similarly protects against overuse of defamation and libel claims by requiring strict proof for any such suit.[130] The First Amendment also provides protection against prior restraint of speech, including censorship of proposed

---

[124] PRIVACY SHIELD FRAMEWORK, *Recourse, Enforcement and Liability*, https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY.
[125] *See* Chapter 3; *see also* 18 U.S.C. § 2518(10)(a); *United States v. Warshak*, 631 F.3d at 282-89 (6th Cir. 2010) (noting that evidence acquired under the Stored Communications Act without a warrant is subject to the exclusionary rule).
[126] *Wong Sun v. United States*, 371 U.S. 471 (1963).
[127] FED. R. EVID. 103 (Explaining how a party can preserve the right to appeal a ruling to admit or exclude evidence at trial).
[128] 18 U.S.C. App III §§ 1-16. For a more detailed discussion of CIPA, please see Chapter 8, Section IV.
[129] *Id.*
[130] U.S CONST. amend. I, *New York Times Co. v. Sullivan*, 376 U.S. 254, 727 (1964) (requiring proof of actual malice "to award damages for libel in actions brought by public officials against critics of their official conduct.").

articles,[131] and it enables the ability to freely publish confidential information even if it was unlawfully obtained and/or shared with the journalist.[132]

[65] Non-governmental privacy advocate organizations in the US use their expertise and resources to pursue systemic change and recourse on behalf of aggrieved individuals.[133] The Electronic Privacy Information Center (EPIC), for example, which is participating in this proceeding, undertakes numerous privacy protective activities, including petitions to the FTC regarding individual harms.[134] The American Civil Liberties Union, Center for Democracy and Technology, Electronic Frontier Foundation, Open Technology Institute, and numerous other non-governmental organizations conduct similar efforts, including assessing and compiling government documents obtained under the Freedom of Information Act.[135] Individuals concerned about their privacy rights can petition any or all of these organizations, or any similar foreign non-governmental organization who may work with these American organizations, who can then work independently or in concert to use their resources and influence to remedy an individual wrong or influence changes in US policies or procedures. The value of the free press and non-governmental organizations in the US represents an important path for privacy remedies for individuals.

III. Additional US Privacy Remedies under Federal Law

[66] Individuals can seek redress for privacy harms from private companies, such as service providers of webmail and social networks, that improperly disclose information to the US government.[136] These service providers have strong incentives to follow the law and their own stated company policies, as violations can result in enforcement actions, costly lawsuits and significant reputational harm to the business. The SCA and Wiretap Act in particular allow for suits against private companies that unlawfully share customer data, which can result in costly damage awards.[137] These risks shape what information companies are willing to share with the government and under what processes.

---

[131] *See New York Times Co. v. United States*, 403 U.S. 713, 717 (1971) ("Both the history and language of the First Amendment support the view that the press must be left free to publish news, whatever the source, without censorship, injunctions, or prior restraints.").
[132] *Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001) ("We think it's clear that parallel reasoning requires the conclusion that a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern.").
[133] COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE (2008) (analyzing US-based privacy advocacy groups).
[134] ELECTRONIC PRIVACY INFORMATION CENTER, *EPIC Administrative Procedure Act (APA) Comments*, EPIC.ORG, https://epic.org/apa/comments/.
[135] AMERICAN CIVIL LIBERTIES UNION, *Section 215 Documents*, https://www.aclu.org/foia-collection/section-215-documents.
[136] For a more detailed discussion of these remedies, see Chapter 7, Section III(A).
[137] A thorough explanation of damages available under the SCA and Wiretap Act are available in Chapter 7, Section III(A).

[67] Federal administrative agencies serve as regulators and enforcers of data subjects' privacy rights for companies under each agency's jurisdiction, including for improper disclosure of electronic communications by the companies to the government. These agencies serve as primary enforcers over their respective areas of expertise, which can overlap. Chapter 7 discusses five of these agencies: the Federal Trade Commission (FTC); Federal Communications Commission (FCC); Consumer Financial Protection Bureau (CFPB); Securities and Exchange Commission (SEC); and Department of Health and Human Services (HHS). I focus on the role of the FTC and its authority under arguably the "single most important piece of US privacy law,"[138] enforcement of unfair or deceptive acts and practices in or affecting commerce.[139]

[68] Under the FTC Act and other statutory authority, the FTC has assumed the role of privacy enforcer of unfair and deceptive practices such as violations of company privacy statements,[140] inadvertent sharing of subscriber email addresses,[141] misleading statements regarding data security practices,[142] misuse and collection of children's data,[143] and spam email practices.[144] The FTC often begins enforcement investigations in response to consumer complaints made directly to the agency, press reports, complaints from business competitors, or from internal FTC research.[145] The FTC can, after an investigation, decide to bring an administrative action before an Administrative Law Judge, whose decision can be appealed to a US federal district court.[146] In practice, the FTC often settles these actions through consent decrees and accompanying consent orders[147] which can include fines and company commitments to improve policies and procedures and submit to future audits and review of privacy practices.[148] These decrees are public documents, which can serve to establish best practices and baseline minimum protections among companies in order to avoid future enforcement.[149] Indeed, Professors Daniel Solove and Woodrow Hartzog state that "today FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States"[150] and that the FTC's "sprawling jurisdiction to enforce privacy" covers what can otherwise appear to be unregulated areas of US commerce.[151] Similar effects exist for the other agencies' enforcement and regulatory activities, as discussed in Chapter 7.

---

[138] *See* SWIRE AND AHMAD, *supra* note 3, at 14.
[139] 15 U.S.C. § 45.
[140] *See* SWIRE AND AHMAD, *supra* note 3, at 17 (discussing *In the Matter of GeoCities, Inc.*).
[141] *Id.* (discussing *In the Matter of Eli Lilly & Co.*).
[142] *Id.* (discussing *In the Matter of Microsoft Corp.*).
[143] *Id*. at 14 (discussing the FTC's authority under the Children's Online Privacy Protection Act).
[144] *Id.* (discussing the FTC's authority under the Controlling the Assault of Non-Solicited Pornography and Marketing Act).
[145] *Id.* at 15.
[146] *Id.*
[147] *See id.*; FEDERAL TRADE COMMISSION, *Cases and Proceedings*, https://www.ftc.gov/enforcement/cases-proceedings.
[148] *See* SWIRE & AHMAD at 15.
[149] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583, 676 (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.
[150] *Id.* at 587.
[151] *Id.* at 588. The 9th Circuit Court of Appeals' August 29, 2016 opinion in *Federal Trade Commission v. AT&T Mobility LLC* found restrictions on the FTC's enforcement jurisdiction regarding companies classified as common carriers, including Internet service providers. *See FTC v. AT&T Mobility*, No. 15-16585, 2016 WL 4501685 (9th Cir. Aug. 29, 2016), https://cdn.ca9.uscourts.gov/datastore/opinions/2016/08/29/15-16585.pdf. While this current

IV. Enforcement under US State Law and Private Rights of Action

[69] State law and state Attorneys General provide additional privacy protections for consumers both in and outside the US. As discussed by Professor Danielle Citron, these Attorneys General have emerged as key privacy enforcers in the US. Chapter 7 offers a detailed case study of California law and enforcement to illustrate this point.[152] The prevalence of plaintiffs' lawyers and private rights of action, along with the significant damages assessed in these actions, have increased the incentive for companies to comply strictly with applicable law. Importantly, state Attorneys General are permitted to investigate petitions from any individual, including EU persons.

V. US Privacy Remedies Concerns in the Irish Data Protection Commissioner's Affidavit

[70] The Irish Data Protection Commissioner (DPC) has filed an affidavit in this case (the "DPC Affidavit") summarizing findings regarding US remedies.[153] The following briefly cites relevant DPC Affidavit statements, then shows where the Court may find discussion of these issues in my Testimony.

[71] The DPC Affidavit states a finding that "the remedies provided by US law are fragmented, and subject to limitations that impact on their effectiveness to a material extent."[154] Chapter 7 acknowledges that US remedies can appear fragmented, and explains how the numerous ways in which US law permits individuals to remedy privacy violations fit together. The complexity of US law can in part be traced to the fact that more than one source of enforcement can exist for any given privacy issue. This division of authority can be beneficial, as it permits private rights of action for individuals, while allowing multiple agencies to police categories of activity on behalf of data subjects.

[72] The DPC Affidavit states that US remedies "arise only in particular factual circumstances," such as intentional violations, and are "not sufficiently broad in scope to guarantee a remedy in every situation in which there has been an interference with [] personal data."[155] As discussed in Chapter 7, Sections I, III(A), some US remedies – as with criminal statutes generally – require intent to show a violation. The scope of individual US remedies is discussed throughout Chapters 7 and 8.

---

ruling may limit the FTC's ability to bring enforcement actions against companies that offer a common carrier service, I believe the Court's decision was incorrect, and it is now being vigorously appealed. For more details on FTC and other administrative enforcement actions, please see Chapter 7, Section III(B).

[152] *See* Chapter 7, Section IV.

[153] *See* Affidavit of John V. O'Dwyer, *Data Protection Comm'r v. Facebook Ireland Ltd.*, No. 2016/4809P (filed July 4, 2016) (H.C.) [hereinafter "DPC Affidavit"].

[154] *Id.* para. 91.

[155] *Id.* para. 92.

[73] The DPC has suggested, as a positive development, that US remedies may be reassessed "in the context of" the Privacy Shield Ombudsman mechanism.[156] Chapter 7, Section I(A)(1) discusses how EU residents can now lodge complaints with an independent Ombudsman regarding US government collection of data – regardless of whether they have been informed that personal data has been collected, and without needing to show intent or actual harm. Chapter 7 also discusses redress avenues against companies that violate privacy rights, charting remedies available specifically to EU citizens (Annex 1) and the substantial amounts plaintiffs have obtained through US privacy litigation (Annex 2).

[74] The DPC Affidavit states a finding that "the 'standing' admissibility requirements of the US federal courts operate as a constraint on all forms of relief available."[157] Chapter 7, Section V provides details about US case developments since *Clapper v. Amnesty International USA Clapper*,[158] mentioned in the DPC's Draft Decision. Chapter 7 more generally discusses avenues US law offers individuals to remedy privacy violations, including: judicial remedies (Chapter 7, Sections I, III(A)); non-judicial remedies such as the PCLOB and the free press (Chapter 7, Section II); administrative-agency remedies via agencies such as the Federal Trade Commission and Federal Communications Commission (Chapter 7, Section III(B)); and the Privacy Shield Ombudsman (Chapter 7, Section I(A)(1)). The doctrine of standing potentially affects judicial remedies, and Chapter 8 discusses the reasons courts in the US and the EU have been cautious about disclosing national security secrets in open court. Remedies such as the Ombudsman, the PCLOB, and the FTC are not subject to such standing limitations.

[75] The DPC's Affidavit also quotes a number of findings about US surveillance law set forth in EU Commission reports published on November 27, 2013.[159] These Commission reports predate the Review Group's reform recommendations, as well as practically all of the post-Snowden reforms to US foreign-intelligence practice my Report discusses. I would generally refer the Court to Chapters 3 (Systemic Safeguards for Foreign Intelligence), 5 (the Foreign Intelligence Surveillance Court), 6 (the Oxford Assessment of Post-Snowden US Surveillance Law), and 7 (US Individual Remedies) for a picture of US foreign intelligence practice as it stands today.

VI. Conclusions on Individual Remedies, with a Caveat

[76] Part 3 of this Summary of Testimony has set forth the multiple ways that individuals, including EU citizens, can achieve remedies in the US for privacy violations. Before turning to

---

[156] *See* Plaintiff's Reply to the Defence of the First Named Defendant, *Data Protection Comm'r v. Facebook Ireland Ltd.*, No. 2016/4809P (filed Sept. 30, 2016) (H.C.), para. 6(1). The DPC states it "could not have had regard to the Privacy Shield Decision in reaching the Draft Decision as same had not yet been implemented at the date of the adoption of the Draft Decision." *Id.*

[157] DPC Affidavit, *supra* note 153, para. 93.

[158] *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013).

[159] *See* DPC Affidavit, *supra* note 153, paras. 48-52 (quoting European Commission, *Communication from the Commission to the European Parliament and the Council*: *Rebuilding Trust in EU-US Data Flows*, COM(2013) 846 (Nov. 27, 2013); and European Commission, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM(2013) 847 (Nov. 27, 2013)).

Part 4, I briefly discuss a caveat about individual remedies in the intelligence setting. The desirability of individual remedies, in intelligence systems, must be weighed against the risks that come from disclosing classified information. In the terms used in Article 8 of the European Convention on Human Rights,[160] the availability of the individual right to privacy is assessed against the necessity in a democratic society of the interests of national security and public safety.

[77] The field of cybersecurity provides an analogy for deciding what types of remedies individuals should have about processing of their information by surveillance agencies. Many of us today are at least somewhat familiar with three types of cybersecurity precautions: (1) do not click on links in emails, because they might be phishing attacks; (2) update your anti-virus software, so viruses will not infect your computer; and (3) have a good firewall, so attackers cannot get into your system. The idea I am suggesting is simple but I believe helpful – be cautious about creating a new vector of attack, such as individual remedies, into a protected system.

[78] A simple example illustrates the sort of harm to national security that could result from individuals' direct access to their data held by an intelligence agency. Suppose a hostile actor, such as a foreign intelligence service, wants to probe the NSA or a Member State intelligence agency. The hostile actor may have Alice use a text service, Bob an email service, and Carlos a chat service. They then file access requests, and only Bob has a file. If so, then the hostile actor has learned something valuable – the email service is under surveillance, but the text and chat services appear not to be. In this example, the individual remedies become a form of cyberattack – the hostile actor can probe the agency's secrets, and learn its sources and methods.

[79] Chapter 8, on Hostile Actors and National Security Considerations, thus explains ways that a hostile intelligence agency or other advanced persistent threat could use individual remedies as a form of cyberattack. It also points out that attacks against intelligence agencies are not hypothetical – they occur every day by the most capable adversaries in the world. In short, restricted access to an intelligence agency's secrets can be seen as a security feature, as well as being a privacy bug.

[80] The Chapter develops an important, related point – both European and US courts have already created doctrines to prevent this sort of attack. In the US, courts in certain instances recognize what is called the "state secrets doctrine," so that judges (while maintaining overall supervision of a case) take care not to let individual litigation become a route of attack on national security secrets. Similar judicial decisions appear to be the norm in Europe, with judges protecting against disclosure or use in open proceedings of national security information. In

[160] In my discussions of Article 8 of the Convention, I am aware of the related portions of other legal instruments – most importantly Articles 7, 8, and 52 of the Charter of the Fundamental Rights of the European Union. *See* Charter of Fundamental Rights of the European Union, 2000 O.J. C364/01 (Dec. 7, 2000) http://www.europarl.europa.eu/charter/pdf/text_en.pdf; *see also* Explanations relating to the Charter of Fundamental Rights, [2007] O.J. C303/17, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2007.303.01.0017.01.ENG.

other words, established law recognizes limits on individual remedies in the foreign intelligence area.

[81] As a lawyer from the US, I do not attempt to state as an expert how these considerations about hostile actor attacks would be judged under EU law. I do offer some observations, however, based on my previous experience with EU law. As discussed in Chapter 2, I worked extensively in the 1990's on the EU right to access, including leading a US delegation to six EU countries to research how the right to access was interpreted in practice. Article 12 of Directive 95/46/EC states the right to access in broad terms, without specifying exceptions. Nonetheless, our research discovered literally dozens of exceptions in practice.

[82] This experience informs my views about the applicability of Article 8 of the European Convention on Human Rights, and Articles 7, 8, and 47 of the EU Charter of Fundamental Rights. As just discussed, Article 8 of the Convention evaluates the availability of an individual right to privacy against the necessity in a democratic society of the interests of national security and public safety. The EU and US decisions limiting disclosures of national security secrets, just discussed, reflect judicial assessment of how to protect both privacy and national security.

[83] In contrast to Article 8 of the Convention, the right to private and family life in Article 7 of the Charter and the right to data protection in Article 8 of the Charter do not state that the rights have derogations for national security, public safety, or other reasons. It would be surprising to me, however, if Articles 7 and 8 were understood to have no derogations, for consideration of national security and other compelling rights and interests. Similarly, Article 47 of the Charter states, without derogations, that "[e]veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article." It would appear logical to me that EU judges would consider the necessity of national security, public safety, and other public interest factors in determining the scope of individual remedies under Article 47.

[84] In summary overall on individual remedies, Part 3 of this Chapter and Chapter 7 describe the numerous individual remedies available in the US for privacy violations, including for violations of the privacy of EU citizens. These individual remedies exist in addition to the much-improved set of systemic safeguards that exist in the US due to reforms since 2001, and especially since 2013. In discussing individual remedies, I have added a caveat about the scope of individual remedies, in intelligence systems, due to the risks that come from disclosing classified information.

[85] I now turn to Part 4, on other considerations. The combination of systemic safeguards, individual remedies, and other considerations should inform any assessment of the adequacy of protections for data transferred from the EU to the US.

PART 4:
The Potential Breadth of the Decision and Assessing the Adequacy of Protections for Transfers to the US

[86] Part 4 of this Summary of Testimony addresses five considerations:

1. The broad effect under US law of a finding that protections against excessive surveillance are inadequate;

2. The broad effect for transborder transfers to other countries of such a finding, including for the BRIC countries (Brazil, Russia, India, and China);

3. The possible effect of an inadequacy finding concerning Standard Contractual Clauses for other lawful mechanisms for transfer of data to countries outside of the EU;

4. The potentially large negative effects on EU economic well-being from such a finding, as stated by EU institutions and Member States, and required under international trade law; and

5. The potentially large negative effects on EU national security and public safety from such a finding, as stated by EU institutions, and contrary to NATO and the goal of protecting mutual security.

I. The Broad US Definition of "Service Providers" Affected by a Ruling

[87] This proceeding would be simpler in certain respects if the effects of an adequacy finding applied only to one or a relatively few companies. As discussed in Chapter 9, however, the relevant US law applies broadly. Any assertion that Section 702 would apply only to a narrow set of companies such as Facebook is inaccurate.

[88] Section 702 applies to data collection from "electronic communications service providers," a term that is defined broadly under US law.[161] US courts have interpreted the relevant definitions to include any company that provides its employees with corporate email or similar ability to send and receive electronic communications. A finding of inadequate protection that applies to Section 702 would thus apply to almost any company with operations in both the EU and US. There is no exception or statutory interpretation that would narrow the potential applicability of a finding of inadequacy with respect to Section 702. To have that impression would not account for the breadth of such a decision.

[89] The EU legal regime as it applies to consent in the employee context means that the broad application of Section 702 may have a particularly strong effect on human resources activities such as internal corporate communications, managing employees, or payroll. EU data protection authorities have been skeptical that individual employees can provide voluntary

[161] 50 U.S.C. § 1881 (defining "electronic communication service provider" to encompass the definition in the Electronic Communications Privacy Act, 18 U.S.C. § 2510). I note that the discussion in Chapter 9 is to cases that have examined ECPA, not FISA. I am not aware of any reason to believe the use of the term in Section 702 is different. I also am not aware of any declassified FISC opinion that states this precise point.

consent to transfers of their personal data outside of the EU.[162] Companies operating in the EU therefore may face significant challenges in obtaining effective consent from an EU employee to transfer of their personal data to other countries, including the US. Thus, if there is a finding of inadequacy of protection in the US for Standard Contractual Clauses, individual consent in the employment context may not provide a practical alternative basis for transfers.

II. The US Has Stronger Systemic Safeguards than the BRIC Countries

[90] I next make some basic comparisons of the surveillance safeguards in the US compared to the important "BRIC" countries – Brazil, Russia, India, and China. The comparison is relevant due to the nature of the inquiry about US adequacy – when personal data is transferred from the EU to the US, are there adequate safeguards against surveillance by the US government? My Testimony has provided details about the many systemic safeguards and individual remedies that are in place against excessive national security surveillance for data that is transferred to the US.

[91] The basic point is simple – suppose that safeguards against surveillance in the BRIC countries are weaker than safeguards in the US. If the US is found inadequate, then logically it would appear that the safeguards in countries with weaker safeguards are also inadequate. Put another way, if the US safeguards are found inadequate, then it would appear that transfers of personal data would have adequate protection only for countries that have *stronger* safeguards than the US.

[92] My analysis indicates that the safeguards in the BRIC countries are clearly less extensive than those in the US.[163] Beginning with China, there is an unmistakable contrast between the pervasive surveillance and information control accompanying the "Great Firewall of China" and the US system of checks and balances under the US Constitution. One recent study described the Chinese approach as "unbounded surveillance," and reported that "the Chinese government has a huge appetite for Internet surveillance and for the technological facility to spy undetectably."[164] A study by European data protection experts analyzed some laws that protect privacy in a

[162] The Article 29 Working Party has indicated that when human resources data transfers occur as "a necessary and unavoidable consequence of the employment relationship," it would be considered "misleading" for employers to use consent as a basis because "[i]f it is not possible for the worker to refuse, it is not consent." Thus, "consent will not normally be a way to legitimise [data] processing in the employment context." *See* Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context* (WP 48), 13 September 2001, at 3, 23, 28, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf. If consent is considered as a basis for transfers, it can be freely withdrawn, which can require employers to respect employee wishes to keep data in the EU. *See id.* at 4 ("Employers would be ill-advised to rely solely on consent other than in cases where, if consent is subsequently withdrawn, this will not cause problems.").

[163] I base my statements here in part on travel to India in 2011 and Russia in 2016; in both cases I met with senior officials on privacy and cybersecurity matters and did extensive research about the national systems. My statements here about all four countries are based on my study of international surveillance and privacy issues over the past two decades, including discussions with experts from each of the countries at conferences and elsewhere.

[164] Ann Bartow, *Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China*, 74 OHIO ST. L.J. 853, 854, 893 (2013), http://digitalcommons.pace.edu/lawfaculty/922.

commercial context, but did not report on any significant safeguards against government access to individuals' communications.[165]

[93] The lack of surveillance safeguards in Russia has been documented in detail by the European Court of Human Rights in the 2015 *Zakharov* case.[166] That case involved the so-called SORM surveillance system in Russia, which provides direct, hardwired access to electronic communications for numerous government agencies: the Federal Security Service, Tax Police, Interior Ministry, Border Guards, Customs Committee, Kremlin Security Service, Presidential Security Service, Parliamentary Security Services, and the Foreign Intelligence Service.[167] The ECHR in the *Zakharov* case held that the SORM program's unrestricted access to telephone communications, without prior judicial authorization, violated Article 8 of the European Convention on Human Rights.[168] As noted in Privacy International's Special Report *Private Interests: Monitoring Central Asia*, "the direct access mandated under the SORM model represents a departure from American and European Lawful Interception protocols and a considerable challenge to the protection of individual human rights."[169]

[94] The legal systems of India and Brazil fall between China and Russia, on the one hand, and the set of systemic safeguards and individual remedies in the US. India has a complex legal system, with laws that vary considerably among its 29 states. Indian surveillance practices after Snowden have a "current state of opacity," with relatively little public documentation of actual communications surveillance practices.[170] There is little reason, however, to believe that India has nearly as robust a system of systemic safeguards as the US: "[C]ommunications surveillance continues to be the exclusive domain of the Executive arm of the Government," and there are "no provisions for judicial or public oversight of the surveillance process."[171] This lack of

---

[165] Paul de Hert & Vagelis Papakonstantinou, European Parliament Directorate General for Internal Policies, *The Data Protection Regime in China: In-Depth Analysis for the LIBE Committee*, PE 536.472 EN, (Oct. 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

[166] *Zakharov v. Russia*, App. No. 47143/06 (Eur. Ct. H.R. 2015), Grand Chamber (Dec. 4, 2015), http://hudoc.echr.coe.int/eng?i=001-159324; *see also* GLOBALVOICES, *As Russia insulates itself from human rights bodies, state surveillance decision looms* (Dec. 17, 2015), https://advox.globalvoices.org/2015/12/18/as-russia-insulates-itself-from-human-rights-bodies-state-surveillance-decision-looms/ [hereinafter "*As Russia Insulates Itself"*].

[167] *See* WORLD POLICY INSTITUTE, *Russia's Surveillance State*, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance; *New powers for the Russian surveillance system SORM-2*, SECURITY AFFAIRS (Aug. 18, 2014), http://securityaffairs.co/wordpress/27611/digital-id/new-powers-sorm-2.html.

[168] *Zakharov v. Russia*, App. No. 47143/06 (Eur. Ct. H.R. 2015), http://hudoc.echr.coe.int/eng?i=001-159324; *see also As Russia Insulates Itself*, *supra* note 166.

[169] PRIVACY INT'L, *Privacy Interests: Monitoring Central Asia* (Nov. 2014), https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf.

[170] WORLD WIDE WEB FOUNDATION, INDIA'S SURVEILLANCE STATE: COMMUNICATIONS SURVEILLANCE IN INDIA (undated, but content indicates publication post June 2013 Snowden disclosures), http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf [hereinafter "INDIA'S SURVEILLANCE STATE"]; Pranesh Prakash, *How Surveillance Works in India*, N.Y. TIMES (July 10, 2013), http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india; *see also* CENTER FOR DEMOCRACY AND TECHNOLOGY, *National Security Standards by Country* (2013), https://govaccess.cdt.info/standards-ns-country.php [hereinafter "*National Security Standards by Country*"]; VODAFONE, *Law Enforcement Disclosure Report: Legal Annex* (June 2014), http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf [hereinafter "*Vodafone Law Enforcement Report*"].

[171] INDIA'S SURVEILLANCE STATE, *supra* note 170, at 49.

judicial or other oversight, and lack of transparency, contrast sharply for instance with the actions of the US Foreign Intelligence Surveillance Court as discussed in Chapter 5.

[95] A detailed 2015 study on Brazil's surveillance practices indicates a system that appears to be closer to the EU and US approaches than the three other BRIC countries.[172] For law enforcement access, Brazil has judicial oversight and statistical reporting, as well as data retention requirements for communications metadata. The study expresses concern that surveillance is "limited in theory but extensive in practice."[173] For intelligence and national security surveillance, "little is known" about the relevant agencies' "operations in Brazil. Moreover, there is almost no information about the oversight exercised by the Joint Commission of the National Congress."[174] Based on this lack of transparency and oversight, it appears difficult to make the case that the systemic safeguards for national security surveillance are stronger in Brazil than for the US.

[96] The four BRIC countries are large and important nations and trading partners of the EU. All have extensive surveillance activities with less transparency and oversight, and fewer overall systemic safeguards and individual remedies, than the US.[175]

[97] The relative lack of safeguards is noteworthy for at least two reasons. First, I have encountered the view that transfers from the EU to the US should be prohibited, due to US surveillance laws, while simultaneously expressing the view that transfers from the EU to other countries, such as China, would be permitted. This reference to China led me to examine the implications of the Chinese safeguards against surveillance, which are less extensive than safeguards in the US.

[98] Second, my experience in global data protection law leads me to the conclusion that the relative lack of safeguards in the BRIC countries holds true for the preponderance of other countries outside of the EU. The role of the US as the "benchmark" for surveillance safeguards, and the relative lack of safeguards in most non-EU countries, has important implications: if the US is held to lack adequate protections against surveillance, then logically there would be lack of adequacy in the BRIC countries and numerous other countries. Only countries whose safeguards are demonstrably stronger than those in the US would appear to have a lawful basis to receive personal data from the EU. The logical import of this conclusion apparently would remove the lawful basis for substantial portions of transborder data flows from the EU.

---

[172] DENNY ANTONIALLY AND JACQUELINE DE SOUZA ABREU, STATE SURVEILLANCE OF COMMUNICATIONS IN BRAZIL AND THE PROTECTION OF FUNDAMENTAL RIGHTS, ELECTRONIC FRONTIER FOUNDATION, 13 (Dec. 2015), https://www.eff.org/files/2015/12/17/brazil-en-dec2015_0.pdf [hereinafter "STATE SURVEILLANCE IN BRAZIL"]; *see also National Security Standards by Country*, *supra* note 170, and *Vodafone Law Enforcement Report*, *supra* note 170.

[173] STATE SURVEILLANCE IN BRAZIL, *supra* note 172, at 22.

[174] *Id.* at 39.

[175] An analysis under Article 47 of the Charter would appear to have these countries lacking the "effective remedies" and review of claims required by an "independent and impartial tribunal." *See* Art. 47, Charter of Fundamental Rights of the European Union, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

III. An Inadequacy Finding for SCCs May Have Implications for Other Lawful Bases for Data Transfers

[99] The current proceeding specifically concerns whether Standard Contract Clauses (SCCs) provide adequate protection, with reference to US surveillance practices. The Draft Decision of the Data Protection Commissioner said that she considered herself "bound by the judgment" in the 2015 *Schrems* case to engage in the current legal proceedings.[176] I understand this statement as the Commissioner seeing a link between the legal treatment of one basis for legal transfer (the Safe Harbor) and another basis for legal transfer (SCCs). Should a Court agree with that link, then there is a possibility that a judgment in the instant proceeding will have implications for other bases for legal transfer.

[100] There are multiple ways that a legal finding about one legal basis for transfer may or may not be relevant to a legal finding about a different legal basis. To begin, I understand the instant proceeding as an opportunity to develop a much more detailed factual record than was before the CJEU in the 2015 *Schrems* case. My Testimony sets forth numerous aspects of US law and practice that were not in the record in the 2015 case. As discussed throughout my Testimony, there are strong reasons to conclude that the system of safeguards in the US for foreign intelligence investigations is stricter and more effective in practice than those in EU countries. The detailed record before the Court in this proceeding thus illustrates how a judicial finding about adequacy under one lawful basis of transfer (Safe Harbor) can be consistent with a different judicial finding about another lawful basis of transfer (SCCs).

[101] If the Court were to find inadequacy in the instant proceeding, this prospect of different adequacy findings could logically occur under other lawful bases such as Privacy Shield or Binding Corporate Rules (BCRs). There are similarities between SCCs, Privacy Shield, and BCRs, such as the announcement in the Privacy Shield that the Ombudsman procedures will apply to data transferred under any of those lawful bases.[177] Also, for data stored in the US, so far as I am aware the same rules apply under Section 702 of FISA and other legal authorities, no matter whether the transfer took place under SCCs, Privacy Shield, or BCRs. On the other hand, there may be important considerations within EU law why a judgment about adequacy under SCCs could lead to a different result than adequacy under other methods of transfer, such as Privacy Shield or Binding Corporate Rules. I do not make any statement about the EU legal question of what effect, if any, a finding about adequacy in the instant proceeding would have on the adequacy of Privacy Shield or BCRs.

[102] With that said, the impact of the current proceeding would vary considerably depending on whether a finding of inadequacy of US surveillance protections applied only to SCCs, or applied more broadly to other bases for lawful transfer. The impact of an inadequacy finding

---

[176] *See* Plaintiff's Reply to the Defence of the First Named Defendant, *Data Protection Comm'r v. Facebook Ireland Ltd*, No. 2016/4809P (filed Sept. 30, 2016) (H.C.), para. 65.

[177] EU-U.S. PRIVACY SHIELD, Annex III.A., 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 (stating that the Ombudsperson will process "requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCRs), "Derogations," or "Possible Future Derogations").

only for SCCs would be smaller than an inadequacy finding that applied also to Privacy Shield and BCRs. Should EU courts over time find that SCCs, Privacy Shield, and BCRs are unavailable, then it is difficult for me to see how to create a lawful basis for many data transfers that currently exist. There are indeed other derogations that permit transfers of data even where the recipient nation lacks adequacy, notably consent. EU data protection authorities, however, have taken a clear stance against widespread use of consent in a variety of settings, including for human resources records,[178] and I am not aware of any other general-purpose way to transfer personal data lawfully.

[103] If over time the CJEU were to find lack of adequacy for all of the transfer mechanisms to the US, then there appears to be limited ways that institutions other than the courts could effectively disagree with or change the finding after the fact. Under the Lisbon Treaty, the decisions of the CJEU have binding effect on the Member States.[179] If the Commission, Member States, or other institutions were to disagree with a CJEU finding of US inadequacy, then the constitutional structure of the EU makes that difficult to implement. Under the US Constitution, Article V creates a process for amendment,[180] and the amendment process has sometimes been used to over-rule US Supreme Court decisions.[181] No similar amendment process amendment process exists now in the EU. My understanding, which is consistent with my discussions with experienced EU lawyers, is that it quite possibly would require a renegotiation of the Lisbon Treaty to counter a CJEU finding of inadequacy of the US surveillance safeguards.[182]

[104] **In short, I make no statement about whether a finding of inadequacy for SCCs would entail a finding of inadequacy for Privacy Shield or BCRs. The discussion here does support the possibility that an inadequacy finding for SCCs may have implications for other lawful bases for data transfers. In the balance of this Testimony, I refer to that broader possibility as a "categorical finding of inadequacy" – a finding of inadequacy that would apply not only to SCCs but also to Privacy Shield and BCRs.** If an inadequacy finding applied only to SCCs, then the effects of the finding may be limited, especially if the opportunity exists to interpret or update Privacy Shield and BCRs for the specific use cases where SCCs have been most helpful to date. If a categorical finding of inadequacy were to

---

[178] The human resources issue is discussed above in Part 4(A) of my Summary of Testimony, in connection with the issue of the wide range of companies whose data transfers are potentially affected by a ruling in this case.

[179] *See generally* TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION, Arts. 19, 251-281, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

[180] *See* U.S. CONST. Art. V. A constitutional amendment can be passed with a super-majority of support, typically two-thirds of both houses of the US Congress, and ratification by three-fourths of the states.

[181] There are at least three examples where a constitutional Amendment over-ruled a US Supreme Court case: (1) the 11th Amendment, concerning suits by citizens of one state against another state, came after *Chisholm v. Georgia*, 2 U.S. 419 (1793); (2) the 16th Amendment, allowing an income tax, came after *Pollock v. Farmers' Loan & Trust Company,* 157 U.S. 429 (1895*);* and (3) the 24th Amendment, abolishing the poll tax, came after *Breedlove v. Suttles*, 302 U.S. 277 (1937).

[182] One other logical possibility is that an ECJ decision could say there is currently inadequacy but it could be cured if the US changed its practices. Any such decision would be similar to a set of instructions of how the US should change its national security practices, which would raise delicate issues of EU/US foreign relations. Going forward, it would also mean the courts would need to update their findings about another nation's overall national security practices, which often involve classified information. That sort of evaluation of a non-Member State practices would involve the courts in challenging questions of the sort historically handled through diplomatic means.

occur, however, it would appear to have significant implications for the overall EU/US relationship, affecting the foreign relations, national security, economic, and other interests of the Member States and the EU itself. I next turn to how such a categorical finding would affect the economic well-being of EU Member States.

IV. Economic Well-Being of the Country

[105] My view is that there would be large economic effects from a categorical finding that the US lacks adequacy due to its surveillance regime. The development of a detailed record in the current proceeding, in my view, provides an opportunity to set forth those economic effects, along with my extensive comments about the nature of the adequacy of the systemic surveillance safeguards themselves.

[106] I do not undertake a statistical analysis of the magnitude of the potential economic effects. Instead, my comments are based on my overall experiences in the field. In considering the economic effects, I briefly discuss EU statements about the importance of the trans-Atlantic economic relationship, before examining international trade considerations.

A. European Union Statements about the Importance of the Transatlantic Economic Relationship

[107] The EU Commission has emphasized the economic importance of the trans-Atlantic relationship and of transborder data flows between the EU and US. The Privacy Shield documents state: "The transatlantic economic relationship is already the world's largest, accounting for half of global economic output and nearly one trillion dollars in goods and services trade, . . . supporting millions of jobs on both sides of the Atlantic."[183] Concerning data flows, the Commission's final Privacy Shield Adequacy Decision states that "the exponential increase in data flows" between the EU and the US is of "critical importance for the transatlantic economy."[184]

[108] EU data protection authorities have agreed. In its review of the draft Privacy Shield documents, the European Data Protection Supervisor stated that the EU-US alliance is "the biggest trading partnership in the world," and that the purpose of its review was "to boost transatlantic relations" so that they could be "stable in the long term."[185] The Article 29 Working Party, while expressing concerns about aspects of the Privacy Shield, agreed that "data

---

[183] EU-U.S. PRIVACY SHIELD, Annex I.1., 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.

[184] 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. 7, 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.

[185] European Data Protection Supervisor, *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, (May 30, 2016), at 2, 12, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf.

transfers that take place between the EU and the U.S. on a daily basis" constitute "a vital part of the economy on both sides of the Atlantic."[186]

[109] EU Member States, in light of the stakes, have also expressed their "strong support" for the Privacy Shield, to create that lawful basis for data flows.[187] The political branches of Ireland, along with major partners such as France, Germany, and the United Kingdom, participated in the Article 31 Committee process to consider the Privacy Shield. The Committee's records show that 24 Member States, representing 96 percent of the EU population, voted in favor of Privacy Shield,[188] with 4 abstentions and none in opposition. Ireland – represented by its Department of Justice and Equality[189] – supported Privacy Shield. In sum, EU institutions and the Member States have clearly indicated the importance of maintaining transborder data flows and fostering the trans-Atlantic relationship.

B. Trade Agreements Including the General Agreement on Trade in Services

[110] There are important provisions in international trade treaties that support privacy protections.[190] In my opinion, a categorical finding of inadequacy of US surveillance safeguards, and blockage of data transfers to the US, would create a significant possibility of a treaty violation.

[111] As is widely understood, the general approach under the World Trade Organization and the General Agreement on Trade and Tariffs is to support free trade and suppress protectionist measures. For that reason, a legal rule that prevents data from leaving a jurisdiction can pose a free trade difficulty – what is the lawful basis for treating transfers to a different country such as the US differently than data sharing within a country?

---

[186] Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision* (WP 238), (Apr. 13 2016) at 12, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

[187] European Commission, Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the adoption by Member States of the EU-U.S. Privacy Shield Privacy Shield, Statement 16/2443 (July 8, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm.

[188] *See* Committee on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Formal vote on Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of protection provided by the EU-U.S. Privacy Shield , V046420/01, CMTD(2016)0868 (July 8, 2016), http://ec.europa.eu/transparency/regcomitology/index.cfm?do=search.documentdetail&ZMd/3IPPHtzAeedC2zZGx1H1ssUUcBMQ0wtPEeDmiVQXV3U4/r7rgJvJWdYwELHg (showing 95% of Member States represented at Art. 31 Committee voted in approval of Privacy Shield).

[189] *See* Summary record of the 71st meeting of the Committee on the Protection of Individuals with regard to the Processing of Personal Data (Article 31 Committee), S046419/01 CMTD(2016)0868 (July, 8 2016), http://ec.europa.eu/transparency/regcomitology/index.cfm?do=search.documentdetail&ZMd/3IPPHtzAeedC2zZGx41KHuMFW2Bq3YHOFmINgVoXV3U4/r7rgJvJWdYwELHg (showing that Ireland's Department of Justice and Equality participated in the Privacy Shield vote); Jedidiah Bracy, *EU Member States approve Privacy Shield*, IAPP.ORG (July 8, 2016), https://iapp.org/news/a/eu-member-states-approve-privacy-shield/ (identifying only Austria, Croatia, Slovenia, and Bulgaria as having abstained from voting on Privacy Shield).

[190] PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 188-96 (1998).

[112] For privacy, the usual answer is that the General Agreement on Trade in Services (GATS) has a specific privacy exception. To provide more scope for nations to enact data protection laws, Article IV of the GATS states:

> Nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures . . . (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: . . . (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.

This language provides a significant legal defense against the claim that a data protection regime violates GATS or the free trade regime more generally.

[113] The data protection exception is limited, however. Article XIV also states the exception is subject "to the requirement that such measures are not applied in a manner which would constitute *a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail*, or a disguised restriction on trade in services." (emphasis added).

[114] There is a factual question as to what constitutes "unjustifiable discrimination between countries where like conditions prevail." In my view, however, this GATS language provides an additional reason to consider how the safeguards in the US compare to both the EU and to other nations, such as the BRIC countries. As discussed in Chapter 6, the Oxford team's finding that the US is the "benchmark" for such safeguards raises a difficulty under the GATS when EU Member States have less thorough safeguards. In addition, the concern about "unjustifiable discrimination" would appear to apply if transfers were allowed to the BRIC or other countries but not to the US.[191]

[115] A categorical finding of inadequacy of US surveillance safeguards thus raises the risk of significant economic effects because of the elimination of lawful transfers, which according to EU institutions are vitally important, and also because of the sanctions that may result from treaty violation under the GATS.

V. National Security

[116] As is true for economic well-being, European institutions have strongly supported the EU/US relationship in the areas of national security, law enforcement, and information sharing for intelligence purposes. The EU Commission has stated: "The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared

[191] A similar consideration is the possible effect of "most favored nation" (MFN) provisions under international trade treaties. The concern would arise where Member States are required to provide the same trade opportunities to an MFN partner (such as the US), but provide the US with less access to EU markets than countries with lesser surveillance safeguards.

values, our security and our common leadership in global affairs."[192] Data flows "are an important and necessary element" of this alliance, not only for economic reasons, but also as "a crucial component of EU-US co-operation in the law enforcement field."[193] Data flows are also critical to "the cooperation between Member States and the US in the field of national security."[194]

[117] This year's EU "Information Sharing Directive" is a recent and clear indication of the importance of the EU/US relationship for fighting international crime and terrorism.[195] That Directive governs information sharing with non-EU countries for counter-terrorism and law enforcement purposes. The Directive declares that the "free flow" of data to third countries such as the US "should be facilitated" for "the prevention of threats to public security."[196] In the wake of this Directive, the EU and US signed the Umbrella Agreement (discussed above) governing data sharing with the US for these purposes. The Dutch Minister who signed the Umbrella Agreement on behalf of the EU stated that the Agreement "symbolises the values the [US] and the [EU] share,"[197] and the Agreement itself describes trans-Atlantic data flows as "critical to prevent, investigate, detect and prosecute criminal offenses, including terrorism."[198]

[118] Similar support for EU/US information sharing and national security come from national security obligations of Member States, such as under the North Atlantic Treaty Organization (NATO). Under Article 3 of the North Atlantic Treaty, members "maintain and develop their individual and collective capacity to resist armed attack" though "continuous and effective self-help and mutual aid."[199] Cybersecurity and cyber defense exemplify the importance of information sharing: "We will continue to integrate cyber defence into NATO operations and operational and contingency planning, and enhance information sharing and situational

---

[192] European Commission, *Communication from the Commission to the European Parliament and the Council*, COM (2013) 846, at 2 (Nov. 27, 2013), http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.
[193] *Id.*
[194] *Id.*
[195] *See* Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, http://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A119%3ATOC&uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG.
[196] *Id.* at Recital (4).
[197] *See* European Council, Press Release 305/16, Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign "Umbrella agreement," (June 2, 2016), http://www.consilium.europa.eu/en/press/press-releases/2016/06/02-umbrella-agreement/ (remarks of Dutch Minister Ard van der Steur, who signed the Umbrella Agreement on behalf of the EU).
[198] *See* Umbrella Agreement, *supra* note 70, at Recital 1, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.
[199] The North Atlantic Treaty, Washington, D.C., April 4, 1949, U.N.T.S. 243, http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

awareness among Allies."[200] Similar national security relationships for information sharing exist among intelligence agencies, including but by no means limited to the Five Eyes countries.[201]

[119] Information sharing for national security and public safety reasons is important in countering terrorist attacks of the sort that have struck Brussels, Paris, and elsewhere in the recent past. Our Review Group report discussed in detail why information sharing about individuals is especially important to counter terrorist threats.[202] Today, both ordinary citizens and terrorists use largely the same devices, software, and computer networks, so surveillance of terrorism suspects often takes place on networks used by ordinary citizens. By contrast, during the Cold War, the most important threats came from nation states such as the Soviet Union, with a far lower likelihood of monitoring the communications of ordinary citizens. This convergence of communication systems used by terrorist suspects and other persons is an important factor, in my view, of what is "necessary in a democratic society" for facing current terrorist threats.

[120] In sum, this discussion shows that a categorical finding of inadequacy would create substantial risks for national security and public safety, be contrary to the clear policies of EU institutions, and also raise issues for Member State treaty obligations. In a period marked by highly visible terrorist attacks within the EU, disruption of information sharing also raises the risk that future terrorist attacks will not be prevented.

PART 5:
Concluding Discussion

[121] This Summary of Testimony explains that the combination of systemic safeguards and individual remedies in the US, in my view, are clearly effective and "adequate" in safeguarding the personal data of non-US persons. Moreover, the Court of Justice of the European Union (CJEU) has announced a legal standard of "essential equivalence" for transfers of personal data to third countries such as the US. Based on my comprehensive review of US law and practice, and my years of experience in EU data protection law, my conclusion is that overall intelligence-related safeguards for personal data held in the US are greater than in the EU. Even more clearly, the US safeguards are at least "essentially equivalent" to EU safeguards. I therefore do not see a basis in law or fact for a conclusion that the US lacks adequate protections, due to its intelligence activities, for personal data transferred to the US from the EU.

[122] This Summary of Testimony discusses the potential breadth of a decision in this proceeding, and makes observations relevant to assessing the adequacy of protections for data transfers to the US. I examine issues in this proceeding under Article 8 of the European

---

[200] Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, Art. 73, September 5, 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[201] A public source of information about the Five Eyes intelligence sharing activities is DAVID ANDERSON, A QUESTION OF TRUST: A REPORT OF THE INVESTIGATORY POWERS REVIEW PRESENTED TO THE PRIME MINISTER PURSUANT TO SECTION 7 OF THE DATA RETENTION AND INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT (June 2015) (UK), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

[202] REVIEW GROUP REPORT, *supra* note 10, at 180-187.

Convention of Human Rights (and related provisions in other EU legal instruments). Article 8 provides that "[e]veryone has the right to his private and family life." It also states: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." I address similar considerations under the Charter's Article 7 (right to private and family life), Article 8 (right to data protection), and Article 47 (right to effective remedy).

[123] In terms of Article 8 of the Convention, in my view based on two decades of experience in US and international privacy and surveillance laws and practices, the systemic safeguards and individual remedies in the US in combination result in necessary actions that are taken "in accordance with law." In light of those safeguards and individual remedies available to EU citizens in the US, I respectfully believe and assert that continued transfers of personal data under Standard Contract Clauses are "necessary in a democratic society" to protect vital interests of the EU, including national security, public safety, and economic well-being.

CHAPTER 2:

BIOGRAPHICAL CHAPTER OF PETER SWIRE

[1] This Chapter, along with providing information on my overall expertise in privacy, focuses on two areas of expertise relevant to the current proceeding – EU data protection law and US surveillance law.

[2] My overall expertise in privacy has developed through more than 20 years of focusing primarily on privacy and cybersecurity issues, as both a professor and senior government official. I have written six books and numerous academic articles, and have testified before a dozen committees of the US Congress. I am lead author of the standard textbook used for the US private-sector privacy examination of the International Association of Privacy Professionals (IAPP).[1] In 2015, the IAPP, among its over 20,000 members, awarded me its Privacy Leadership Award. For government service, under President Clinton I was Chief Counselor for Privacy in the US Office of Management and Budget, the first person to have US government-wide responsibility for privacy issues. Under President Obama, I was Special Assistant to the President for Economic Policy in 2009-10. In 2013, after the initial Snowden revelations, President Obama named me as one of five members of the Review Group on Intelligence and Communications Technology (which I refer to as the "Review Group"). My full CV is available at www.peterswire.net.

[3] Section I of this Chapter describes my years of experience with EU data protection law. In 1998, I was lead author of the book "None of Your Business: World Data Flows, Electronic Commerce, and the EU Privacy Directive."[2] Under President Clinton, I participated in the negotiation of the EU/US Safe Harbor. Since that time, I have continued to work on EU data protection issues. In December 2015, when the Belgian Privacy Agency held a forum on the effects of the initial *Schrems* decision, I was the sole American from the private sector asked to participate.

[4] Section II of this Chapter describes my years of experience in US surveillance law. Under President Clinton, I chaired White House working groups on both encryption and wiretap law. In 2004, I wrote the most-cited law review article on foreign intelligence law.[3] As a member of the Review Group, I was co-author of our 300-page report, which was re-published as a book by the Princeton University Press.[4] The Review Group was told in 2014 by the Obama

---

[1] Peter Swire & Kenesa Ahmad, *U.S. Private Sector Privacy: Law and Practice for Information Privacy Professionals*, INT'L ASSOC. OF PRIV. PROF. (2012), https://iapp.org/media/pdf/certification/cippus-us-private-sector-ch3.pdf.

[2] PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EU PRIVACY DIRECTIVE (1998).

[3] Peter 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 [hereinafter Swire 2004 Paper]. The citation count is based on a search on the term "foreign intelligence" in the Social Science Research Network, www.ssrn.com.

[4] PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY (2014), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Administration that 70 percent of our 46 recommendations have been adopted in letter or spirit, and additional recommendations have since been adopted.[5]

[5] To the best of my knowledge, I am the only person to have authored both a book on EU data protection law as well as one on US surveillance law. This Chapter highlights my experiences in both areas, including how these experiences have informed and shaped my views on these issues over more than two decades.

I. Expertise in EU Data Protection Law

[6] I provide a chronological discussion of my experience in EU data protection law.

[7] (1) Student of European Community law (1980-81). I graduated from Princeton University in 1980, summa cum laude and Phi Beta Kappa, and then spent the 1980-81 academic year studying in Brussels on a Rotary Scholarship. While there, I took classes at the Institut d'Études Européennes, in French, on European Community Law. This early experience sparked my interest in the topic, and assisted my later research in EU data protection law.

[8] (2) Early research on privacy and Internet law (1993-96). Based on my long-standing interest about the intersection of technology and law, I wrote my first article on the law of the Internet in early 1993.[6] By 1996, I decided to focus on privacy law, and published an article on the relative strengths of markets, self-regulation, and legal enforcement for privacy protection.[7] The article was published in the proceedings of a conference of the US Department of Commerce, which was studying privacy in part because the EU Data Protection Directive was adopted in 1995.

[9] (3) Lead author of book on EU Data Protection Directive and its effect on EU/US relations (1996-98). In 1996, the Brookings Institution asked me to be lead author on a book that was published in 1998 as "None of Your Business: World Data Flows, Electronic Commerce, and EU Privacy Directive." I personally did the great majority of the research and writing for the book. Among other things, the book included interviews with leading data protection experts, including Peter Hustinx (then leader of the Dutch Data Protection Authority (DPA), and later the first European Data Protection Supervisor (EDPS)) and Giovanni Buttarelli (now the EDPS).

[10] In essence, the book described in careful detail what actual data flows went from the EU to the US, and how they differed by sector, such as medical, financial, human resources, e-commerce, and so on. The book then analyzed what exceptions to the Directive might enable data flows, if there were no general finding that the US had "adequate" privacy protections. The book pointed out numerous practical challenges in applying the relatively abstract terms of the Directive to specific factual settings. The book also proposed policy options. Based on my

---

[5] For instance, the Obama Administration announced in 2016 that it will split the National Security Agency (an intelligence agency) from United States Cyber Command (a military command), consistent with a Review Group recommendation.

[6] Peter Swire, *Public Feedback Regulation: Learning to Govern in The Age of Computers, Telecommunications, and the Media* (1993) (unpublished), http://peterswire.net/archive/feedback-93.htm.

[7] Peter Swire, *Markets, Self-Regulation, and Legal Enforcement in the Protection of Personal Information*, SOC. SCI. RESEARCH NETWORK, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=11472.

participation in the EU/US negotiations, the book was an important source of information and policy ideas for what became the Safe Harbor agreement, signed in 2000.

[11] (4) Project on EU/US Model Contract Clauses (1997-98). During this period I worked with Alan Westin, often considered the founder of privacy law studies in the US, on a project about how to draft model contract clauses for EU/US data flows. Standard contractual clauses are the legal instrument whose adequacy is being challenged in the current case.

[12] (5) Leader of US government delegation to EU on privacy issues (1997-98). While I was writing the book, governmental discussions continued about the rules for lawful transfers of data flows from the EU to the US. In 1997-1998, the US Government asked me to lead two official trips to Europe, accompanied by a representative of the US State Department and US Department of Commerce. We visited data protection officials and other privacy experts in Belgium, France, Germany, the Netherlands, Sweden, and the United Kingdom.

[13] The purpose of the effort illustrates an important theme, in my experience, about the EU and US in privacy protection. We were studying in detail how a fundamental principle of EU data protection law, the right to access, operated in practice in Europe. The right to access is often expressed in broad terms, with statements saying that individuals always have the right to access to information processed about them.[8] In fact, our discussions in Europe showed literally dozens of exceptions to the absolute version of the right to access. To pick one example, we learned that university students did not have a right to get copies of their examinations – professors are of course permitted to keep the exam questions secret, so they can use the questions in later years. The results of this research fed directly into the Safe Harbor negotiations; because the US government had developed a nuanced understanding of the right to access, the Safe Harbor agreement provided quite a bit of detail on the right of access. This detail helped ensure fair treatment of Safe Harbor companies, so they could use the same exceptions that were used by companies in the EU.

[14] In my view, this example provides a valuable lesson for the current case, where Article 47 of the Charter of Fundamental Rights of the European Union states: "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal." As with the right to access, my understanding of EU law is that there are many exceptions in practice, notably including for intelligence-related activities. As with the right to access in the 1990's, a fundamental question in this proceeding is whether the US provides "adequate" safeguards. I believe a fair assessment of "adequacy" for intelligence issues should include a nuanced understanding of the exceptions that exist in practice under EU law.

[15] (6) Chief Counselor for Privacy, including the Safe Harbor negotiations (1999-2001). At the beginning of 1999, I took a leave of absence from my position as a law professor and became

[8] Article 12 of Directive 95/46/EC states broadly, "Member States shall guarantee every data subject the right to obtain from the controller" information about the data subject held by the controller, and this access shall be "without constraint at reasonable intervals and without excessive delay or expense." Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, at Art. 12, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Article 13 provides a list of exceptions. Our research uncovered numerous additional types of exceptions applied in practice.

the Chief Counselor for Privacy in the US Office of Management and Budget. In this role, I had US government-wide responsibility for privacy policy. I met regularly with the US Commerce Department officials who were leading the negotiations of the Safe Harbor (David Aaron and Barbara Wellbery) as well as with EU officials involved in the negotiations. The Safe Harbor agreement was approved by the European Commission in July 2000.

[16] (7) Continued work on EU Data Protection issues prior to the Snowden leaks (2001-13). In early 2001, I returned to my position as a law professor, teaching and researching on EU data protection as well as other privacy and cybersecurity topics. I consulted with a law firm, including about trans-border data flows. I traveled to Europe periodically, such as to speak at Data Protection Commissioner's conference in Switzerland and what I believe was the first conference in Europe on the intersection of privacy issues with competition law. My continued scholarship on EU data protection law included a lengthy article on the new right to data portability in 2012.[9]

[17] In 2012-13 I served as global co-chair for the Do Not Track process of the World Wide Web Consortium, which sought to create a consensus standard for enabling consumer choice about personal data used on web sites. Throughout this process, I engaged regularly with European regulators and civil society experts, as we sought to craft a standard that would be useful in the EU, the US, and globally.

[18] (8) President Obama's Review Group on Intelligence and Communications Technology (2013-14). I provide more detail below on surveillance issues in the Review Group report. Concerning expertise in EU data protection in particular, I was the member of the Review Group who led our meetings related to EU issues. Our meetings included representatives of the EU Commission, EU Parliament, Member States, and Data Protection Authorities, as well as a meeting with the now-deceased EU surveillance expert Caspar Bowden.

[19] Our report made multiple recommendations relevant to the EU, including: Privacy Act reform, now enacted in the Judicial Redress Act; Mutual Legal Assistance reform; new rules for US surveillance of foreign leaders; and new rules for authorizing sensitive intelligence collections, such as in allied countries. Presidential Policy Directive 28 (PPD-28), which makes privacy an integral part of US intelligence collection, is consistent with our analysis and recommendations.

[20] (9) EU-related activities since the Review Group (2014-present). Since the Review Group finished in early 2014, I have continued to work extensively on EU data protection issues. I am an annual speaker at the Computers, Privacy, and Data Protection conference in Brussels each January. I am leading a research project on mutual legal assistance reform funded by the Hewlett Foundation, including study of EU procedures for gathering and sharing evidence for criminal and foreign intelligence investigations. The fifth article in that project will be published in 2017 by the Emory Law Journal, on ways that both the EU and US are stricter than each other for the privacy of government requests for information. Consistent with university rules, I serve

[9] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335 (2013), http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3550&context=mlr.

as Senior Counsel to Alston & Bird, where I provide privacy and security counsel, and am currently participating in a series of webinars on how organizations may comply with the General Data Protection Regulation that takes effect in 2018.

[21] (10) Activities related to litigation between Max Schrems and Facebook. At the time of the initial *Schrems* decision in October 2015, I wrote two widely read analyses for the International Association of Privacy Professionals blog.[10] The Belgium Privacy Authority, on behalf of the Article 29 Working Party, held a forum in December 2015 on trans-Atlantic and related issues post-Schrems. Outside of the US government, I was the only US speaker. I submitted 42-page testimony entitled "U.S. Surveillance Law, Safe Harbor, and Reforms since 2013." I wrote this as an independent professor and private citizen, with no compensation for the work. Many of the conclusions in the December testimony are the same as discussed in the testimony in this case.

[22] In January, I participated in an extended discussion on a panel with Max Schrems, as part of the Computers, Privacy, and Data Protection conference in Brussels. That discussion is available online.[11] During that trip to Europe and afterwards, as a private citizen, I met with the senior EU and US officials in connection with the Privacy Shield negotiations.

II. Expertise in US Surveillance Law

[23] I provide a chronological discussion of my experience in US surveillance law.

[24] (1) Chair of White House Working Group on Encryption (1999). Perhaps the most controversial privacy issue in the US in the 1990's was encryption – more specifically, whether to allow export of strong encryption software. Because encryption historically had been used primarily in military settings, the US historically limited the export of strong encryption. As a professor in the 1990s, I critiqued these export controls, believing that strong encryption was essential to effective security and privacy on the Internet.[12]

[25] When I entered the White House in early 1999, I chaired the White House Working Group on Encryption, which was reviewing the administration's export control policy.[13] In September of that year, the administration announced a major change in position, generally allowing export of strong encryption. Along with the US Attorney General and other senior

---

[10] Peter Swire, *Solving the Unsolvable on Safe Harbor – the Role of Independent DPAs*, IAPP PRIVACY PERSPECTIVES (Oct. 13 2015), https://iapp.org/news/a/solving-the-unsolvable-on-safe-harbor-the-role-of-independent-dpas; Peter Swire, *Don't Strike Down the Safe Harbor Based on Inaccurate Views About U.S. Intelligence*, IAPP PRIVACY PERSPECTIVES (Oct. 5 2015), https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law.

[11] *Privacy in the EU and US: A Debate between Max Schrems and Peter Swire*, SOUNDCLOUD, https://soundcloud.com/justin-hemmings-44462987/privacy-in-the-eu-and-us-a-debate-between-max-schrems-and-peter-swire.

[12] In 1997, I co-authored a paper with Michael Froomkin and Lawrence Lessig critiquing proposed limits on the use of domestic encryption. *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. AND TECH. L. REV. 416, 439 n. 26 (2012) (discussing the paper).

[13] A White House "Working Group" of this sort includes senior officials from various parts of the White House and various agencies who have expertise or an interest in an issue. Where there is no consensus at the Working Group level, issues are raised to more senior officials, including the President if necessary.

officials, I spoke at the White House announcement, emphasizing the importance of strong encryption for security and privacy.[14]

[26] My period as chair of the Working Group gave me experience working with senior officials in the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), the Department of Defense (DOD), and other federal agencies. A central debate is whether strong encryption helps national security by creating effective privacy and cybersecurity, or instead hurts national security because it can make surveillance more difficult. Based on years of scholarship and experience with these issues, I continue to believe that strong encryption is the correct outcome, to promote privacy and overall security.[15] Participating in these debates, however, made me sensitive to the deeply felt concerns of law enforcement and foreign intelligence experts. In the 1999 debates, my own views matched the eventual US government position, supporting encryption. I was impressed, however, with the sincerity and public-spiritedness of the law enforcement and intelligence officials who participated in the process.

[27] (2) Chair of White House Working Group to Update Surveillance Law (2000). In 2000, I was asked to lead a White House Working Group to update wiretap laws for the Internet era. The assignment came from John Podesta, then Chief of Staff to President Bill Clinton, and co-author himself of a book about email privacy in the early 1990's. The Working Group included intelligence and law enforcement lawyers from agencies including the NSA, the Central Intelligence Agency (CIA), the FBI, the Department of Justice, and others. After months of detailed deliberations, we completed draft legislation, which was submitted to Congress. (The legislation did not pass before President Clinton left office in early 2001).

[28] I believe acting as Chair for this process prepared me well for a perspective that strongly supports privacy and civil liberties in surveillance, while being intensely mindful as well of what is necessary in a democracy to protect national security and public safety. As the nation's lead privacy official, I looked for ways to strengthen safeguards. As the official responsible for crafting an overall legislative proposal, I needed to listen carefully to the concerns of other officials. I sought to separate blanket statements from agency officials of "we need broader authorities" from well-argued statements of "we need this authority for these specific reasons, and we can comply with the proposed safeguards." Reporting directly to the President's Chief of Staff, I felt a personal responsibility to create a proposal that would achieve the public good. In the years since, as these debates have continued, I have continued to feel that responsibility.

[29] (3) Continued surveillance research including "The System of Foreign Intelligence Surveillance Law" (2004-13). Based on my time in the White House, I believed that the Foreign Intelligence Surveillance Act (FISA) and related laws were critical to the issues of liberty and

---

[14] Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire (Sept. 16, 1999), WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, http://intellit.muskingum.edu/cryptography_folder/encryption2.htm.

[15] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy Before the S. Comm. on the Judiciary*, 114th Cong. (2015) (statement of Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business Georgia Institute of Technology), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf.

democratic governance, yet very poorly understood. This belief led me to write a lengthy law review article, published in 2004, on "The System of Foreign Intelligence Law."[16] According to the Social Science Research Network, this remains the most-cited academic article about foreign intelligence issues. In the course of this research, I conducted extensive interviews with officials who had been involved in the drafting and implementation of the nation's intelligence laws.

[30] Many of the themes from the 2004 article are evident in Part 2 of my Testimony, which emphasizes the importance of systemic safeguards for foreign intelligence activities, rather than a focus on individual remedies. The 2004 article made multiple policy recommendations. Due to the efforts of many individuals in the years since, including myself, quite a few of these reforms have now been adopted. The Annex to this Chapter lists the approximately 10 reforms first proposed in print in my 2004 article, and how they have been implemented today.

[31] As shown in my CV, I have continued to work extensively on surveillance law issues over the years, testifying in Congress multiple times, and writing articles such as "Privacy and Information Sharing in the War Against Terrorism."[17]

[32] (4) President Obama's Review Group on Intelligence and Communications Technology, 2013-14. I had a unique opportunity to deepen my knowledge of US surveillance law and practice as one of the five members of President Obama's Review Group. The other members had great expertise: Richard Clarke, who had been top anti-terrorism and cybersecurity advisor to both Presidents Clinton and George W. Bush; Michael Morell, former Deputy Director of the CIA, with 30 years of experience in the intelligence community; Geoffrey Stone, former Dean of the University of Chicago Law School and noted civil liberties expert; and Cass Sunstein, former senior government official and the most frequently cited American legal scholar.

[33] President Obama directed us to advise him on an approach "that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust and reducing the risk of unauthorized disclosure."[18] We were granted security clearances that enabled us to access any information we thought relevant to the task. We visited the headquarters and interviewed senior officials at the major intelligence agencies, including NSA Director Keith Alexander. We had high-quality staff and received the briefings we requested from officials in many agencies. We conducted meetings with experts outside of the US government and received public comments.

[34] When we completed our report of over 300 pages in late 2013, we met with President Obama to discuss the 46 recommendations. The five members were unanimous in the report and recommendations. To build trust, we decided that the entire report would be made public. The government reviewed our report only to ensure that there was no leak of classified information – we had complete editorial control.[19]

---

[16] Swire 2004 Paper, *supra* note 3.
[17] Peter Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 260 (2006), http://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1195&context=vlr.
[18] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *About the Review Group on Intelligence and Communications Technologies*, https://www.dni.gov/index.php/intelligence-community/review-group.
[19] As with the Review Group Report, my submission to the court is reviewed by the US government to ensure that no classified information is leaked, but I retain complete editorial control.

[35] The Review Group report had an important effect on debates about US surveillance. The report received front-page coverage in the major US newspapers. Princeton University Press decided to reprint our report as a book, the first time a US government report had received such reprinting since the 9/11 Commission. Privacy and civil liberties groups were generally very positive about the report.

[36] In terms of impact, President Obama made a speech about surveillance reform in January 2014. The Review Group members were told at that time that 70 percent of our recommendations had been accepted in letter or spirit. Additional reform happened over time. Notably, the USA FREEDOM Act passed Congress in 2015, and its major provisions closely tracked the Review Group recommendations.[20]

[37] In conclusion on the Review Group, the process convinced me of the importance of creating legal regimes for surveillance that are informed by multiple perspectives, including civil liberties, privacy, national security, effects on foreign relations, and economic effects. Access to top-secret information is clearly helpful, in my view, to overall judgments about how to achieve goals such as privacy and civil liberties consistent with national security and public safety. As a member of the group, I felt fortunate to be able to test ideas and draft recommendations while being informed by the years of intelligence community experience of Richard Clarke and Michael Morell. If I thought an idea seemed promising, and they thought it was workable in practice, then I felt more confident supporting a reform. Without access to their insights, I think our recommendations would have been less persuasive to the Administration, Congress, and the public.

[38] In conclusion on my overall background, I understand that my duty as an expert is to assist the Court as to matters within my area of expertise and this overrides any duty or obligation that I may owe to the party whom I have been engaged by or to any party liable to pay my fees. I have dedicated my professional efforts for more than two decades to understanding privacy and related issues as both a professor and government official. Drawing on my experience in both US surveillance law and EU data protection law, I seek to explain the former in ways that will form an accurate basis for the Court in developing the latter.

[20] The close fit between the USA FREEDOM Act and the Review Group recommendations is discussed in Peter Swire, *The USA Freedom Act, the President's Review Group, and the Biggest Intelligence Reform in 40 Years*, IAPP PRIVACY PERSPECTIVES (June 8, 2015), https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years.

Annex to Chapter 2

Reforms Recommended in my 2004 Article titled "The System of Foreign Intelligence Surveillance Law" and Corresponding US Reforms

[39] In my 2004 article on "The System of Foreign Intelligence Surveillance Law," [21] I provided recommendations for reforming the system in the wake of the 9/11 attacks and the passage of the USA PATRIOT Act. For many of these, the recommendations were first proposed in print in that article; ten of the recommendations made in the paper have been substantially adopted.

[40] As information about my background, I include the details of this paper to illustrate that I have been a public critic of US surveillance practices, especially in the wake of the USA-PATRIOT Act passed in 2001. As information about the development of US surveillance law, the discussion here shows that the US has made significant pro-privacy reforms since the 2004 critique. Based on these reforms, as stated in Chapter 6, my assessment of the US system has developed to one in line with the Oxford team that finds the US to be the global "benchmark" for transparent principles, procedures, and oversight for national security surveillance.[22]

[41] The recommendations from the 2004 paper which have been implemented are: (1) ending the bulk collection power under Section 215 to obtain records other than tangible items; (2) the inclusion of a more adversarial system in the Foreign Intelligence Surveillance Court (FISC); (3) the addition of adversary council in Foreign Intelligence Surveillance Court of Review (FISCR) appeals; (4) greater use of Inspector General oversight after the fact; (5) changing the expansion of the 'gag rule' with National Security Letters (NSLs); (6) improved record-keeping of NSLs; (7) notification to data subjects after the FISA surveillance had concluded; (8) disclosure of legal theories accepted by the FISC; (9) formalization of minimization procedures used by the FISC; and (10) ensuring surveillance under FISA is focused on foreign intelligence.

I. Ending the Bulk Collection Power under Section 215 to Obtain Records Other Than Tangible Items

[42] *Recommendation from 2004 paper—Ending the bulk collection power under Section 215 to obtain records and other tangible objects*: In 2004, I wrote,

> "The Patriot Act substantially expanded the government's power to obtain records and other tangible objects through Section 215. The Patriot Act expanded the scope of FISA orders to records in important ways: the order can extend beyond travel records to "any tangible things including books, records, papers, documents, and other items"; and the records may be those of any person, rather than requiring "specific and articulable facts that the person to whom the records

[21] Swire 2004 Paper, *supra* note 3.

[22] Ian Brown, et al., *Towards Multilateral Standards for Surveillance Reform* (2015) at 19, https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf.

> pertain is a foreign power or an agent of a foreign power." One consequence of the statutory change is the apparent permission of a FISA order to encompass entire data bases, rather than the specific records of the target of an investigation.[23]

My 2004 recommendation was that this new Section 215 power should be ended.

[43] *Reform:* The USA FREEDOM Act ended the bulk collection practice under Section 215 for collection of "tangible things" (including phone records).[24]

II. The Inclusion of a More Adversarial System in the FISC

[44] *Recommendation from 2004 paper—The inclusion of a more adversarial system in the FISC:* In 2004, I wrote, "The details of FISC procedures are not publicly available. Department of Justice officials seeking FISA orders present documents to the FISC judges. Members of the Department's Office of Intelligence Policy and Review serve certain staff functions for the Court. There is no adversarial process, however, and no one is specifically tasked with critiquing the order as it is sought." My recommendation was that

> Congress may . . . wish to authorize specifically the creation of a 'Team B' or 'devil's advocate' role within the FISC process. As a related possibility, the statute might specifically authorize the FISC judges to ask for that sort of representation in a particular case where they believe it would assist the Court. The devil's advocate would presumably have gone through full security clearance. For instance, the advocate might serve for a period of years and then return to other functions within the Department of Justice. Oversight could be available after the fact to determine the extent to which this innovation has proved helpful.[25]

[45] *Reform:* The USA FREEDOM Act authorized the creation of a group of independent experts, called *amici curiae* (friends of the Court), to brief the FISC on important cases.[26] The law instructs the FISC to appoint an *amicus curiae* for a matter that, in the opinion of the court, "presents a novel or significant interpretation of the law."[27] The court retains some discretion on when to appoint an *amicus curiae*, but the clear intent of the statute is that independent lawyers with security clearances shall participate before the FISC in important cases. This reform provides the opportunity for independent views to be heard by the FISC for important cases, so that the assertions of government officials can be carefully tested before the judges. The statute does not precisely state what role the *amicus curiae* should play, but the first criterion for selection is "expertise in privacy and civil liberties."[28] The FISC has named six expert lawyers as *amici curiae*, including a professor as well as lawyers who have been involved in civil

---

[23] *Id.* at 78.
[24] 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, § 103 (2015), https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf (amending 50 U.S.C. § 1861(b)(2), 1861(c)).
[25] Swire 2004 Paper, *supra* note 3, at 93-94.
[26] USA FREEDOM Act § 401.
[27] *Id.*; 50 U.S.C. § 1803 (i)(2).
[28] USA FREEDOM Act § 401; 50 U.S.C. § 1803 (i)(3).

liberties and foreign intelligence matters either in prior government service or in private practice.[29]

III. The Addition of Adversary Counsel in FISCR Appeals

[46] *Recommendation from 2004 paper—The addition of adversary counsel in FISCR appeals*: In *2004*, I wrote, "The first case appeals to the FISCR showed a clear gaps in existing procedures. *Amici* were permitted by the Court to submit briefs. There was no statutory mechanism, however, that permitted *amici* or any party opposing the government to participate in an oral argument." My recommendation in 2004 was, "[e]ven if some or all of the oral argument of the Department of Justice is closed for security reasons, there can be a separate session involving *amici* or other parties. In addition, where *amici* or other parties are represented by a person with security clearances, then the FISCR might decide to include cleared counsel into the entire argument."[30]

[47] *Reform:* The USA FREEDOM Act provides that an *amicus* may be appointed for proceedings in the FISCR, under the same provision as the *amicus* is appointed for the FISC. The statute also makes a provision for the appointment of an *amicus* in the event that a case is appealed from the FISCR to the United States Supreme Court.[31]

IV. Greater Use of Inspector General Oversight after the Fact

[48] *Recommendation from 2004 paper—Consider greater use of Inspector General oversight after the fact*: In 2004, I wrote, "There can be greater after-the-fact review of the operation of FISA from within the Justice Department or other elements of the intelligence community." My recommendations was for a statute that required oversight by the existing Office of the Inspector General or a special office that could be created for foreign intelligence activities. The report of that oversight could be given to the Congressional Intelligence and Judiciary Committees.[32]

[49] *Reform*: The Privacy and Civil Liberties Oversight Board (PCLOB) is an independent agency that was established by the Implementing Recommendations of the 9/11 Commission Act in 2007 and fully constituted as an executive agency in 2013.[33] The PCLOB is an independent oversight agency focused on privacy, with the same independent structure as the Federal Trade Commission. In my experience, EU data protection experts have often praised the structure of an independent agency focused on privacy. 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 Top Secret/Special Compartmentalized Information security clearances and investigate and report on

---

[29] *See* U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Amici Curiae*, http://www.fisc.uscourts.gov/amici-curiae. For a recent report on how one such *amicus curiae* case has worked in practice, *see* Tim Cushing, *FISA Court's Appointed Advocated Not Allowing Government's 'National Security' Assertions To Go Unchallenged*, TECHDIRT.COM (Dec. 11, 2015), https://www.techdirt.com/articles/20151210/08175733048/fisa-courts-appointed-advocate-not-allowing-governments-national-security-assertions-to-go-unchallenged.shtml.

[30] Swire 2004 Paper, *supra* note 3, at 94.

[31] 50 U.S.C. § 1803.

[32] Swire 2004 Paper, *supra* note 3, at 98.

[33] *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *What is the Privacy and Civil Liberties Oversight Board?* https://www.pclob.gov/.

the counterterrorism activities of the US intelligence community. The board is tasked with providing oversight and advice on the topics related to protecting the nation from terrorism while ensuring that privacy and civil liberties are protected.

[50] In addition, every agency involved in intelligence work, both military and non-military, has an Inspector General. Individuals serving within these agencies are able to report waste, fraud, and abuse in a way that the sensitive material remains confidential and yet the problems are brought to the attention of the appropriate authorities. These IGs meet with the Intelligence Community Inspector General on a regular basis to address concerns that span more than one organization.[34]

V. Reduced Use of the "Gag Rule"

[51] *Recommendation from 2004 paper—Reduced use of the "gag rule":* In 2004, I detailed my concern about non-disclosure orders, often called the "gag rule," applying to Section 215 orders and National Security Letters,[35] authorized under Section 505 of the USA PATRIOT Act.[36] These statutory provisions made it illegal for individuals or organizations to disclose that they had been asked by the government to provide documents or other tangible objects.[37] In my paper, I stated, "This 'gag rule' is an unjustified expansion of a special rule for wiretaps, and is contrary to the rules that have historically applied to government requests for records."[38] My recommendation in 2004 was that the special circumstances that justify the "gag rule" for ongoing wiretaps – namely, an investigation is still open – not be permitted for NSLs and Section 215 orders.

[52] *Reform:* In 2006, the 'gag rule' provision in the USA PATRIOT Act was set to sunset,[39] unless additional legislation was passed by Congress.[40] During the time period when Congress was considering its actions related to the 'gag rule,' two recipients of NSLs filed suits in federal

---

[34] OFFICE OF THE INSPECTOR GEN. OF THE INTELLIGENCE COMMUNITY, OCTOBER 1, 2015 – MARCH 31, 2016 SEMIANNUAL REPORT TO THE DIRECTOR OF NATIONAL INTELLIGENCE, 8 (2016) (describing the Intelligence Community Inspector General Forum, where the IC Inspector General meets with other Inspectors General on a regular basis), https://www.dni.gov/files/documents/ICIG/ICIG-SAR-UNCLASS-OCT15-MAR16.pdf.

[35] In 2004, I described the little-known tool of NSLs that had been significantly expanded by the USA PATRIOT Act. For those unfamiliar with the term, I described the expansion of the scope of NSLs under Section 505 of the USA PATRIOT Act as essentially the foreign intelligence corollary to administrative subpoenas for criminal investigations. After the USA PATRIOT Act, NSLs applied to "an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709(b). NSLs are permitted under the Electronic Communications Privacy Act for telephone and electronic communications records, 18 U.S.C. § 2709; the Right to Financial Privacy Act for financial records, 12 U.S.C. § 3414(a)(5)(A); and the Fair Credit Reporting Act for credit records, 15 U.S.C. § 1681u.

[36] Section 215 of the USA PATRIOT Act expanded the sweep of FISA orders to compel production of business records and other tangible items. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act of 2001), Pub. L. No. 107-56, § 215 (2001), https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/content-detail.html (amending 50 U.S.C. §§ 1862, 1862).

[37] *See, e.g.*, 18 U.S.C. § 2709(c).

[38] Swire 2004 Paper, *supra* note 3, at 83.

[39] Sunset provisions expire unless reauthorized by Congress.

[40] *See* CHARLES DOYLE, CONG. RESEARCH SERV., RL 32186, USA PATRIOT ACT SUNSET: PROVISIONS THAT EXPIRE ON DECEMBER 31, 2005 (June 29, 2005), http://www.fas.org/sgp/crs/intel/index.html.

court to challenge the validity of the government requests.[41] These lawsuits brought media attention to the fact that the Federal Bureau of Investigation (FBI) had significantly increased the number of NSLs after the passage of the USA PATRIOT Act – from a small number before 2001 to over 30,000 a year after its passage.[42] During this time, I urged that the 'gag rule' for NSLs and Section 215 orders should either be restricted, with oversight by FISC, or that the relevant portions of the USA PATRIOT should be allowed to expire.[43]

[53] In 2006, the 'gag rule' provision of the USA PATRIOT Act was allowed to sunset. Congress then amended, in a pro-privacy direction, the secrecy provisions applying to NSLs, so that: (1) a recipient was allowed to consult an attorney and challenge the request; (2) the nondisclosure was no longer automatic, but required the government official to certify that disclosing the request may result in danger to national security, interference with an ongoing criminal investigation, or danger to life or personal security of any person; (3) the Attorney General must annually report and make public the number of requests per year for information; and (4) the Department of Justice Inspector General must complete an audit detailing information about the NSLs.[44]

[54] Shortly after, Inspector General reports sharply criticized practices of the FBI related to NSLs.[45] In 2007, the Department of Justice adopted substantial oversight and reform of NSLs to address these concerns, and this oversight regime remains in effect.[46]

[55] Consistent with the 2004 article, and as recommended by the Review Group, President Obama announced that the indefinite secrecy of these government requests would change. As of 2015, the FBI now presumptively terminates NSL secrecy for an individual order when an investigation closes, or no more than three years after the opening of a full investigation.

---

[41] *See Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004); *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005). Both plaintiffs who filed suit used a pseudonym that is well-known in US law – John Doe.

[42] Peter Swire, Testimony before the Senate Judiciary Comm., Subcomm. on the Constitution, "Responding to the Inspector General's Findings of Improper Use of National Security Letters by the FBI" (Apr. 11,2001) https://www.judiciary.senate.gov/imo/media/doc/swire_testimony_04_11_07.pdf; Andrew E. Nieland, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1202, 1202-03 (2007), http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=3073&context=clr.

[43] *See* 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.

[44] *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, §§ 115-19 (2006), https://www.congress.gov/bill/109th-congress/house-bill/3199/text?overview=closed.

[45] *See* DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (Mar. 2007), https://oig.justice.gov/special/s0703b/final.pdf.

[46] *See* DEP'T OF JUSTICE, *Fact Sheet: Department of Justice Corrective Actions on FBI's Use of National Security Letters* (Mar. 20, 2007), https://www.justice.gov/archive/opa/pr/2007/March/07_nsd_168.html. These practices were reviewed by the Inspector General in 2008, 2010, and 2014. *See* DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (Mar. 2008), https://oig.justice.gov/special/s0803b/final.pdf; DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS (Jan. 2010), https://oig.justice.gov/special/s1001r.pdf; DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF PROGRESS IN IMPLEMENTING RECOMMENDATIONS AND EXAMINATION OF USE IN 2007 AND 2009 (Aug. 2014), https://oig.justice.gov/reports/2014/s1408.pdf.

Exceptions are permitted only if a senior official determines that national security requires otherwise in the particular case and explains the basis in writing.[47]

VI. Improved Record-Keeping on the Use of National Security Letters

[56] *Recommendation from 2004 paper: Improved record-keeping on the use of National Security Letters (NSLs)*: In 2004, I wrote of my concern that there appeared to be no statutory requirements of any record-keeping about the use of NSLs. My 2004 recommendation was to enact such statutory requirements.[48]

[57] *Reform:* The USA FREEDOM Act requires the Office of the Director of National Intelligence to annually make publicly available on its website the number of NSLs issued and the number of requests for the information contained in the NSLs.[49] In addition, the USA FREEDOM Act guarantees the right of those subject to national security orders to publish detailed statistics.[50] The companies can report statistics in a number of categories, such as content, non-content, and NSLs. Notably, the companies can report ranges of "the total number of all national security process received," including NSLs and orders under FISA.[51] They can also report ranges of "the total number of customer selectors targeted under all national security process received."[52]

VII. Notification to Data Subjects after the FISA Surveillance Had Concluded

[58] *Recommendation from 2004 paper—Consider providing notice of FISA surveillance significantly after the fact*: In 2004, I wrote about notice to the person under surveillance. "For domestic wiretaps, the Fourth Amendment generally requires prompt notice to the target after the wiretap is concluded. For national classified information, even top secret information, there are declassification procedures with presumptions of release to the public after a stated number of years. Yet, anomalously, for FISA the surveillance remains secret permanently." My recommendation in 2004 was that "[s]erious consideration should be given to changing the permanent nature of secrecy for at least some FISA surveillance. Procedures can be created similar to declassification procedures . . . . The threat of eventual declassification may serve as an effective check of temptations to over-use FISA powers for political or other improper ends."[53]

---

[47] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform 2015 Anniversary Report – Strengthening Privacy and Civil Liberties Protections*, IC ON THE RECORD (2015), http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[48] Swire 2004 Paper, *supra* note 3, at 79.
[49] USA FREEDOM Act, Pub. L. No. 114-23, § 603(b) (2015).
[50] *Id.* § 604.
[51] *Id.* §§ 604(a)(3)(A), (4)(A).
[52] *Id.* §§ 604(a)(3)(B), (4)(B).
[53] Swire 2004 Paper, *supra* note 3, at 98.

[59] *Reforms:* NSLs can now be revealed by the companies, usually after three years.[54] In addition, the USA FREEDOM Act provides declassification procedures for FISC opinions. These opinions are then publicly posted on IC on the Record.[55]

VIII. Disclosure of Legal Theories Accepted by the FISC

[60] *Recommendation from 2004 paper—Disclosure of legal theories accepted by the FISC*: In 2004, I wrote that this is important for public knowledge concerning new legal theories or interpretations adopted by the FISC. My recommendations was that "a statute could require notice to Congress and/or the public of new legal arguments presented to FISC."[56]

[61] *Reform:* Under the USA FREEDOM Act, orders of the court that involve substantial interpretations of law must either be declassified or summarized and then made publicly available on the Internet.[57]

IX. Formalization of Minimization Procedures Used by the FISC

[62] *Recommendation from 2004 paper—Formalization of minimization procedures used by the FISC:* The 2004 article analyzed one FISC opinion that had been declassified, which showed a concern by the judges that the statutory requirement that surveillance be minimized was not being met in practice. My recommendation in 2004 was that "having enforced minimization procedures is a long-established way to focus the surveillance on where it is justified, but not to have open-ended surveillance." [58]

[63] *Reform:* Presidential Policy Directive 28 (PPD-28), announced in January 2014, addressed minimization procedures. The retention requirements and dissemination limitations in PPD-28, applying to non-US persons, are consistent across agencies and similar to those for US persons.[59] For retention, different intelligence agencies 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.[60] For dissemination, there is an important provision applying to non-US persons: "personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted." [61]

---

[54] 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].
[55] USA FREEDOM Act, Pub. L. No. 114-23, § 602 (2015).
[56] Swire 2004 Paper, *supra* note 3, at 97.
[57] 50 U.S.C. §1872(b).
[58] Swire 2004 Paper, *supra* note 3, at 95-96.
[59] The agency procedures create new limits on dissemination of information about non-US persons, and require training in these requirements.
[60] There are exceptions to the five-year limit, but they can apply only after the DNI considers the views of Office of the Director of National Intelligence (ODNI) Civil Liberties Protection Officer and agency privacy and civil liberties officials. *See Signals Intelligence Reform 2015 Anniversary Report*, *supra* note 47.
[61] PPD-28, *supra* note 54, at § 4(a)(i).

X. Ensuring Surveillance under FISA is Focused on Foreign Intelligence Purposes

[64] *Recommendation from 2004 paper—Focusing surveillance on foreign intelligence purposes:* In 2004, I wrote about comments that I had heard in public from knowledgeable persons suggesting that there has been ongoing expansion of who was considered an "agent of a foreign power." My concern was to ensure that FISA surveillance be limited to foreign intelligence purposes. My recommendation was that the public needed more information to know how to best address the treatment of those that might fall within the definition of an "agent of a foreign power."[62]

[65] *Reform:* The administration has clearly issued guidelines about limiting surveillance to foreign intelligence purposes. PPD-28 requires paying attention to the privacy of non-US persons and focusing surveillance only on agents of foreign power for legitimate intelligence purposes. PPD-28 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." It adds: "Privacy and civil liberties shall be integral considerations in the planning of US signals intelligence activities." [63]

[66] In sum, my writings after the USA PATRIOT Act of 2001 contained many criticisms of the US surveillance system. Over time many, although by no means all, of the recommendations in the 2004 paper have been adopted. Multiple other intelligence reforms have also been adopted since 2004. This history speaks to the ability of the US system to consider and make important reforms to its surveillance practices and safeguards. As discussed further in the next Chapter, the US today has an extensive system of safeguards for foreign intelligence activities, with an overall effectiveness in my view that is as strict as or stricter than in other countries, including EU countries.

[62] Swire 2004 Paper, *supra* note 3, at 76-78.
[63] PPD-28, *supra* note 54, at § (1)(b).

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.

CHAPTER 4:

SYSTEMIC SAFEGUARDS FOR LAW ENFORCEMENT

[1] This Chapter describes safeguards in the US criminal justice system, as contrasted with the safeguards for foreign intelligence investigations discussed in Chapter 3. As discussed elsewhere in the Testimony, a wiretap or other government collection of electronic communications in the US takes place primarily either under law enforcement or foreign intelligence legal authorities.[1] For collection in the US, Executive Order 12,333 does not apply.[2]

[2] This Chapter first provides an overview of US criminal procedure, highlighting the numerous safeguards built into the Constitution's Bill of Rights. Drawing on my current academic research, it then discusses eight ways in which the safeguards in the US are usually more substantial than the safeguards that apply within the EU.

I. Overview of US Criminal Procedure

[3] The criminal justice system in the US was shaped by the experience of the generation that fought the American Revolution in the 1770s and 1780s. This generation rallied against what it considered violations of their fundamental rights by the British King George III. The US Constitution, and especially the Bill of Rights (the first ten amendments), provides numerous safeguards against the government in criminal cases. These safeguards include:

1. The Fourth Amendment prohibits unreasonable searches or seizures, and generally requires probable cause of a crime, and a warrant overseen by an independent magistrate.[3]

2. The Fifth Amendment prohibits compelled testimony against oneself, provides protections of a grand jury, prohibits two trials for the same crime, and assures due process generally.[4]

[1] When these searches occur under a mandatory order, they follow either the foreign intelligence or law enforcement regime. Section 1802(a) of Title 50 of the U.S. Code 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.

[2] To be explicit, my assumption in writing this Testimony is that the Court is considering the adequacy of protection for data that is transferred to the US, and not for data that remains in the EU. Based on that assumption, I focus my analysis on the legal rules that apply to data transfers. By contrast, Executive Order 12,333 applies to data collected outside of the US.

[3] U.S. CONST. amend. IV ("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.").

[4] *Id.* amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.").

3. The Sixth Amendment assures the right to a speedy and public jury trial, to be informed of the nature of the accusation, to confront adverse witnesses, and to have legal counsel.[5]

4. The Eighth Amendment protects the individual against excessive bail, and against cruel and unusual punishments.[6]

[4] These rights apply to both US persons and non-US persons facing a criminal trial in the US. In the over two centuries since the US Constitution went into effect, the Supreme Court has elaborated on many of these rights, such as the right of an individual to a lawyer supplied by the state if the defendant cannot afford a lawyer.

II. Eight Specific Safeguards in US Law Enforcement Investigations

[5] As part of my ongoing academic research, I am now in the editing stage of two articles. The Emory Law Journal article is entitled "Why Both the EU and the U.S. are Stricter than Each Other for the Privacy of Government Requests for Information."[7] The Wisconsin International Law Review article is entitled: "A Mutual Legal Assistance Case Study: the United States and France."[8]

[6] The Emory Law Journal article describes how the EU is "stricter" (more substantial), especially in having a comprehensive approach to data protection – the current Data Protection Directive, and the upcoming application of the General Data Protection Regulation for commercial data and the new Directive on law enforcement data processing.[9] In my experience, this relative "strictness" of the EU with respect to data protection, as measured by the comprehensiveness of the written law, is widely accepted.

---

[5] *Id.* amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.").

[6] *Id.* amend. VIII ("Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.").

[7] I presented the symposium version of this research in March 2016, before I was aware that I would be asked to participate in this case. The main points in the draft article and this Chapter are the same as those in the March symposium presentation. DeBrae Kennedy-Mayo, a Research Associate at Georgia Tech, is co-author for this law review article.

[8] My co-authors and I agreed to write the article, and drafted the article, before I was aware that I would be asked to participate in this case. The co-authors are Justin Hemmings, who until recently was a Research Associate at Georgia Tech, and Suzanne Vergnolle, a French doctoral student in comparative privacy law who was resident at Georgia Tech in 2015-16.

[9] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89, http://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A119%3ATOC&uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG.

[7] My research supports the less-widely understood conclusion that the US is "stricter" (more substantial) than the EU in multiple respects in the area of criminal procedure safeguards. Specifically, the Emory Law Journal article identifies eight ways in which the US often or usually exceeds the EU protections:

A. Oversight of searches by independent judicial officers;

B. Probable cause of a crime as a relatively strict requirement for both physical and digital searches;

C. Even stricter requirements for government use of telephone wiretaps and other real-time interception;

D. The exclusionary rule, preventing prosecutors' use of evidence that was illegally obtained, and civil suits;

E. Other legal standards that are relatively strict for government access in many non-search situations, such as the judge-supervised "reasonable and articulable suspicion" standard under ECPA;

F. Transparency requirements, such as notice to the service provider of the legal basis for a request;

G. Lack of data retention requirements for Internet communications; and

H. Lack of limits on use of strong encryption.

A. Oversight of Searches by Independent Judicial Officers

[8] Standard practice in the US is that search warrants are issued by a judge, who is a member of the judiciary and not part of the executive branch. Federal judges have strong legal guarantees of independence – Article III of the US Constitution guarantees that federal judges have lifetime tenure, and cannot have their salaries reduced.[10]

[9] This review by an independent judge, separate from the executive branch, is far from universal under European legal systems. Approximately half of the Member States lack review by an independent judge when the government seeks to engage in surveillance.[11] As discussed in

[10] U.S. CONST. art. III. More specifically, the constitutional text provides that federal judges retain their positions during "good behaviour," which means in practice that they have lifetime tenure except in extraordinary circumstances, notably when Congress impeaches the individual judge. *Id.*; *see* Walter F. Pratt, *Judicial Disability and the Good Behavior Clause*, 85 YALE L.J. 706 (1976), http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1164&context=law_faculty_scholarship.

[11] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights, Safeguards, and Remedies in the European Union* at 52 (Nov. 2015), http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf [hereinafter FRA Report]. Even in the United Kingdom, which shares a common law history with the US, the independent judiciary plays a far smaller role in overseeing criminal investigations than in the US. The Regulation of

our Wisconsin International Law Journal article, French public prosecutors typically combine the prosecutorial and judicial roles when determining what evidence to gather for a criminal prosecution.[12]

B. Probable Cause of a Crime as a Relatively Strict Requirement for Both Physical and Digital Searches

[10] Most important for surveillance issues, the Fourth Amendment limits the US government's ability to conduct searches and seizures, and warrants can issue only with independent review by a judge. The Fourth Amendment governs more than simply a person's home or body; its protections apply specifically to communications, covering a person's "papers and effects."[13] In criminal prosecutions, the law enforcement officer must determine whether the Fourth Amendment requires a warrant to conduct a search, or whether it is an instance where a lesser requirement will satisfy the reasonableness requirement of the Fourth Amendment.[14] If law enforcement officers are incorrect in their assessment, the evidence collected may be excluded from evidence in a criminal trial.

[11] The search warrant is issued by a neutral magistrate, a judge, only after a showing of probable cause that there is incriminating evidence in the place to be searched. Probable cause that a crime has been committed must be established by the law enforcement officer by "reasonably trustworthy information" that is sufficient to cause a reasonably prudent person to believe that an offense has been or is being committed or that evidence will be found in the place that is to be searched.[15] In the warrant, the law enforcement officer is required to list, with specificity, the items to be searched and/or seized.[16]

C. Even Stricter Requirements for Government Use of Telephone Wiretaps and Other Real-time Interception

[12] In U.S. law, the real-time interception of electronic data is recognized as holding the greatest privacy risks, and consequently an order authorizing such interception requires a

---

Investigatory Powers Act 2000, c. 23, § 5 (U.K.), http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf. The FRA Report identifies five Member States that engage in the collection of signals intelligence (collection that, at least in the initial stage, targets large flows of data and not an individual). None of these Member States – France, Germany, the Netherlands, Sweden, and the United Kingdom – has a judicial body involved in the approval of signal intelligence. FRA Report at 55, Table 5.

[12] Peter Swire, Justin Hemmings & Suzanne Vergnolle, *Mutual Legal Assistance Case Study: The United States and France*, WISC. INT'L L.J. (forthcoming 2016) [hereinafter *Mutual Legal Assistance Case Study*].

[13] U.S. CONST. amend. IV ("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] In this context, the search is considered to be reasonable if the law enforcement obtained a valid warrant before the search was conducted. DANIEL J. SOLOVE & PAUL SWARTZ, INFORMATION PRIVACY LAW (4th ed. 2015).

[15] *Brinegar v. United States*, 338 U.S. 160 (1949). U.S. Supreme Court cases may be found at https://www.supremecourt.gov/opinions/opinions.aspx or https://supreme.justia.com/.

[16] *Horton v. California*, 496 U.S. 128 (1990). *See* DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 117-18 (2009) http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

heightened standard of proof. Wiretaps are understood as requiring "probable cause plus," with requirements before the courts permit real-time interception:

1. An interception order requires "a particular description" of both the "nature and location of the facilities from which or the place where the communication is to be intercepted" and "the type of communications sought."[17]

2. The application for an interception order must explain "whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or be too dangerous."[18] Failure to exhaust alternate, less-intrusive means of obtaining the same information can result in the denial of an application for an interception order.[19]

3. The application must specify the period of time during which the interception will take place, or a reason why the applicant has probable cause to believe no termination date should be set because additional covered communications will continue to occur.[20] Minimization rules apply so non-relevant communications are not authorized by the wiretap.[21]

4. There are multiple rounds of review within the Department of Justice before a wiretap request can go to a judge – magistrates on their own motion cannot approve a wiretap.[22]

[13] The judge must make a determination in favor of the government on all of these factors to issue an order permitting the interception.[23] Once the order is approved, the government is responsible for complying with minimization procedures. Specifically, the order is to be executed as soon as possible, is to be conducted in such a way as to minimize the incidental collection of communications not subject to the order, and is to be terminated once the communication authorized under the order is obtained.[24] Within 90 days of the termination of the order, the individual who was searched must be notified by the court of the existence of the order.[25]

---

[17] 18 U.S.C. § 2518(1)(b).
[18] *Id.* § 2518(1)(c).
[19] *Id.*
[20] *Id.* § 2518(1)(d).
[21] *Id.* § 2518(5); *see, e.g.*, *United States v. Rivera*, 527 F.3d 891, 904-05 (9th Cir. 2008), https://casetext.com/case/us-v-rivera-33 (describing the government's minimization efforts).
[22] 18 U.S.C. § 2518(1); *see also* 18 U.S.C. § 2510(9) (defining an approving judge as "(a) a judge of a United States district court or a United States court of appeals, and (b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications").
[23] *Id.* § 2518(3). If the request is denied, the court must notify the individual who was the target of the request within 90 days of the denial. *Id.* § 2518(8)(d).
[24] *Id.* § 2518(6).
[25] *Id.* § 2518(8)(d).

D. The Exclusionary Rule, Preventing Prosecutors' Use of Evidence that Was Illegally Obtained, and Civil Suits

[14] In the US criminal law area, individual remedies exist to address evidence obtained during a search that was illegally conducted. In a criminal trial in the US, the courts enforce constitutional rights by excluding evidence that the government obtains illegally.[26] In addition, the courts bar evidence that is "the fruit of a poisonous tree" – additional evidence similarly cannot be used in court if it is derived from an illegal search.[27] Since the 1960s, this "exclusionary rule" has served as an important practical motivation for police officers to follow the rules for searches and seizures.

[15] With regard to civil remedies, an individual who has been the subject of a search that violated the Fourth Amendment can file a lawsuit seeking monetary damages.[28] When the law enforcement officials conducting the search are state or local employees, the individual files a civil rights suit pursuant to 42 U.S.C. § 1983.[29] In a Section 1983 claim, the plaintiff can recover compensatory damages and reasonable attorney's fees. The courts have permitted suits by US citizens and non-US citizens living in the US. [30] In short, the US exclusionary rule, backed up by the "fruit of the poisonous tree" doctrine and civil remedies, provides clear individual remedies against illegal searches.

[16] The adversarial system in the US makes this remedy quite different than the laws in many European countries. For example, in the French system, a search only needs to be necessary to establish the "truth," and any evidence "necessary to establish the truth" can be presented to the bodies investigating and ultimately prosecuting the crime.[31]

E. Other Legal Standards that are Relatively Strict for Government Access in Many Non-Search Situations, such as the Judge-Supervised "Reasonable and Articulable Suspicion" Standard under ECPA

[17] Under the Electronic Communications Privacy Act (ECPA), categories of information that do not require probable cause have historically been available to the government when a judge is

---

[26] *Mapp v. Ohio*, 367 U.S. 643 (1961). In addition to exclusion from evidence under the Fourth Amendment, certain statutes, such as the Wiretap Act, provide for exclusion of evidence for violation of the statutory requirements. *See* 18 U.S.C. § 2518(10)(a).

[27] *Wong Sun v. U.S.*, 371 U.S. 471 (1963).

[28] SOLOVE & SWARTZ, *supra* note 14; *see* 18 U.S.C. § 2518(10)(a).

[29] In addition to § 1983 claims, certain federal statutes provide for a basis for a civil suit. *See* 18 U.S.C. § 2511(4)(a); 18 U.S.C. § 2701(b).

[30] Under § 1983, an aggrieved person is "any citizen of the United States or other person within the jurisdiction thereof." 42 U.S.C. §1983; *see also Plyler v. Doe*, 457 U.S. 202 (1982); *Graham v. Richardson*, 403 U.S. 365 (1971); Martin Schwartz, *Section 1983 Litigation*, FEDERAL JUDICIAL CENTER 27 (2014), https://www.casd.uscourts.gov/Attorneys/CJAAppointments/SiteAssets/docs/FJCSection1983Outline.pdf [hereinafter *Section 1983 Litigation*]. Because Section 1983 claims do not extend to instances where the law enforcement officials conducting the search were federal officers, the United States Supreme Court has recognized an implied remedy known as a *Bivens* claim, so named for the 1971 case in which the claim was first discussed. *See Bivens v. Six Unknown Agents*, 403 U.S. 388 (1971). Generally, the same legal principles and procedures apply in a *Bivens* claim as in a § 1983 claim. *Id.*

[31] For a full comparison of these concepts in French and US laws, *see Mutual Legal Assistance Case Study*.

satisfied that reasonable suspicion exists to believe that the data is relevant to an ongoing criminal investigation based on "specific and articulable facts" presented by the government.[32] This requirement of reasonable and articulable suspicion means that the government must meet the touchstone of the Fourth Amendment's requirement for reasonableness, but does not require a search warrant because the level of intrusion is considered lower than that in a full search.[33]

[18] More recently, federal appellate courts have interpreted ECPA to say that requests under Section 2703(b) (content of communications) do require a probable cause warrant.[34] Some magistrates have placed even further limitations on obtaining content, such as the length of time the content can be retained and limits on searching within a computer for all the files in that computer.[35]

[19] Compared with the approaches in France and other EU countries, the analysis is similar to that provided for the probable cause standard. Once again, an independent judge in the US must make the decision whether the legal standard has been met for the government to access the evidence.

F. Transparency Requirements, such as Notice to the Service Provider of the Legal Basis for a Request

[20] US law and practice is to have clear notice in the judge's order to produce evidence of the legal basis for the order, for instance by citing the specific statutory provision under which the order is issued.[36] This notice enables the recipient of the order to research the lawful basis, to help determine whether there are reasons to challenge the order. By contrast, it is my understanding that companies that receive requests for electronic evidence in many EU and other jurisdictions lack this information about the legal basis for the evidence request.

---

[32] 18 U.S.C. § 2703(d).

[33] The standard derives from *Terry v. Ohio*, 392 U.S. 1 (1968), which established the reasonable and articulable suspicion test for brief police stops of individuals. For one discussion of the relative role of *Terry*, probable cause, and other standards, *see* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 21–47 (2007).

[34] *See e.g., United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), http://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf (holding the Fourth Amendment prevents law enforcement from obtaining stored email communications without a warrant based on probable cause); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012), https://casetext.com/case/united-states-v-ali-5 ("[I]ndividuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider.").

[35] *See United States v. Ganias*, 755 F.3d 125, 134 (2d Cir. 2014), https://casetext.com/case/united-states-v-ganias ("Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools."); *see also Matter of Black iPhone 4*, 27 F. Supp. 3d 74, 78 (D.D.C. 2014), https://casetext.com/case/in-re-in-re-iphone (holding the government "must be more discriminating when determining what it wishes to seize, and it must make clear that it intends to seize *only* the records and content that are enumerated and relevant to its present investigation").

[36] 18 U.S.C. § 2703(b).

G. Lack of Data Retention Rules for Internet Communications

[21] Data retention requirements have been a prominent feature of European debates about how to achieve privacy protections consistent with law enforcement and national security goals. In 2006, the EU promulgated a Data Retention Directive, which required publicly available electronic communications services to retain records for an extended period of time, for purposes of fighting serious crime.[37] For instance, for email and other electronic communications, the communications services were required to retain "the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication."[38] In the *Digital Rights Ireland* case, the European Court of Justice struck down that Directive due to privacy concerns related to excessive access to the retained data and lack of assurances that the records would be destroyed at the end of the retention period.[39] In the wake of that judgment, a number of EU Member States have reinstated modified data retention requirements for telephone and Internet communications.[40]

[22] By contrast, the US does not require data retention for email or other Internet communications. Internet data retention bills have been introduced in Congress, but have not come close to passage.[41] The Federal Communications Commission has issued rules concerning retention of telephone records for up to 18 months.[42] Those rules apply only to "telephone toll records," which are a diminishing portion of all communications, as users increasingly rely on non-telephone Internet communications and often have unlimited phone calls, so toll records are no longer required for billing purposes.

[23] In light of the significant privacy concerns explained in the *Digital Rights Ireland* case, the presence of data retention rules in the EU and their general absence in the US support the view that the absence of such rules is a significant check on the power of government in both law enforcement and foreign intelligence investigations.

H. Lack of Limits on Use of Strong Encryption

[24] At the time of this writing in October 2016, there have been calls for new limits on strong encryption in a growing number of EU countries, including a joint press conference by the

---

[37] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[38] *Id.* at Art. 5(1)(b).

[39] C-293/12, *Digital Rights Ireland v. Minister of Commc'ns*, 2014 E.C.R. I-238, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.

[40] Federico Fabrinni, *Human Rights in the Digital Age: The European Court of Justice Ruling in Digital Rights Ireland and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUM. RTS J. 65 (2015), http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf.

[41] *See* CENTER FOR DEMOCRACY & TECHNOLOGY, *Resources on Data Retention* (Sept. 26, 2012), https://cdt.org/insight/resources-on-data-retention.

[42] 47 C.F.R. § 42.6.

Interior Ministers of France and Germany.[43] In the United Kingdom, in addition to relatively strict rules relating to encryption in the Regulation of Investigatory Powers Act of 2000,[44] limits on end-to-end encryption are included in the proposed Investigatory Powers Bill, which has passed most of the hurdles to passage.[45] In my view and the view of many other experts, such limits on the use of strong encryption pose serious threats to user privacy.[46]

[25] Debates about the use of strong encryption have also occurred recently in the US, most prominently expressed by FBI Director James Comey in the controversy about encryption of the Apple iPhone.[47] The US historically permitted use of strong encryption within the country but limited exports of strong encryption through export control laws. The bulk of these export controls were eliminated in 1999.[48] Based on my extensive experience with encryption policy in the US, I believe legislation limiting the use of strong encryption has a low likelihood of passage.[49] Meanwhile, a number of EU Member States retain stricter laws governing encryption than the US, including France and Hungary.[50] Indeed, US-based technology companies have taken a global position of leadership on use of strong encryption, bolstering the likelihood that encryption-enabled privacy protections will continue to develop in the US.

III. Conclusion

[26] Based on my academic research and other experience, it is a complex task to assess precisely where the US and EU provide stricter safeguards concerning government criminal investigations. This Chapter seeks to inform the more general question of whether the US has "adequate" or "essentially equivalent" safeguards to the Member States of the EU for government access to information about a defendant or other data subject.

---

[43] Natasha Lomas, *Encryption under fire in Europe as France and Germany call for decrypt law*, TECHCRUNCH, (Aug. 24, 2016) https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/.

[44] *See* Bert-Jaap Koops, *Crypto Law Survey, Overview per country, Version 27.0*, CRYPTOLAW.ORG (Feb. 2013) http://www.cryptolaw.org/cls2.htm.

[45] Tirath Bansal, *Investigatory Powers Bill: Rushed through under Cover of Brexit*, COMPUTERWEEKLY.COM (July 13, 2016), http://www.computerweekly.com/news/450300206/Investigatory-Powers-Bill-rushed-through-under-cover-of-Brexit.

[46] *See, e.g.*, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy Before the S. Comm. on the Judiciary*, 114th Cong. (2015) (statement of Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business Georgia Institute of Technology), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf; Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by requiring government access to all data and communications*, MIT COMP. SCI. AND ARTIF. INTEL. LAB. (July 6, 2015), http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[47] Lev Grossman, *Inside Apple CEO Tim Cook's Fight with the FBI*, TIME MAG. (Mar. 17, 2016), http://time.com/4262480/tim-cook-apple-fbi-2/.

[48] Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire, WHITE HOUSE, OFFICE OF THE PRESS SEC'Y (Sept. 16, 1999), http://www.peterswire.net/archive/privarchives/Press%20briefing%20Sept.%2016%201999.html.

[49] Swire in 1999 chaired the White House Working Group on Encryption when the US repealed most of the export controls on export of strong encryption. Since then, Swire has written extensively on encryption law and policy. *See, e.g.*, Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416 (2012), http://stlr.org/volumes/volume-xiii-2011-2012/encryption-and-globalization/.

[50] *See* Bert-Jaap Koops, s*upra* note 44.

[27] The Chapter has described how the creation of the US itself derived in significant measure from an insistence on protecting the rights of individuals in the criminal justice system. That tradition of the Bill of Rights remains in effect today.

[28] The Chapter has also documented eight ways in which the US usually or generally has stricter protections than EU Member States. In the Emory Law Journal article, we call these eight "plus factors," ways that an assessment of the US system should provide additional points – "plus factors" – compared to the EU approach. Critics of the US approach have sometimes listed specific safeguards that exist in an EU country but not in the US and have found these missing pieces to be relevant to an overall assessment of "adequacy" or "essential equivalence." My point here is that the US has significant, and often constitutional, safeguards that usually are lacking in the EU. In my view, a fair comparison of the adequacy of the two systems should carefully consider such additional factors.

CHAPTER 5:

THE US FOREIGN INTELLIGENCE SURVEILLANCE COURT

[1] In 1978, the Foreign Intelligence Surveillance Act (FISA) created a new court exclusively devoted to overseeing government surveillance: the Foreign Intelligence Surveillance Court (FISC). The FISC was born of a fundamental political decision that "[w]iretaps and electronic surveillance for foreign intelligence purposes, conducted within the US," should only be done with approval from a judge.[1] The members of the FISC serve as the judge, as a legislatively-established check by Congress on earlier executive branch claims that it had inherent authority to conduct national security wiretaps.[2]

[2] FISA provided that FISC procedures were generally conducted in secret and *ex parte* (without notice to or participation by the person under surveillance). These rules flowed from efforts to ensure that surveillance targets were not tipped off in advance, and to prevent diplomatic incidents.[3] This history of secrecy meant – as I wrote in 2004 – that "[t]he details of FISC procedures are not publicly available," known only to the "Department of Justice officials" who practiced before the court.[4]

[3] That is no longer true. In recent years, both the FISC and the Obama Administration have carefully and thoughtfully declassified numerous FISC decisions, orders, and opinions, often along with the legal briefing and government testimony underlying them.[5] The FISC itself has disclosed its rules of procedure and its standard review procedures for government surveillance applications. This information is now available on the Internet, but to date there has not been any systematic, published assessment of these newly released materials. This Chapter reports on what the newly declassified materials show.

[4] This Chapter draws on the newly released materials and my experience in foreign intelligence. In general, the materials show evidence that the FISC today provides independent and effective oversight over US government surveillance. Whatever general conclusions one draws about the overall effectiveness of the FISC, the newly released materials show far stronger oversight than many critics have alleged. The Chapter is divided into four sections:

---

[1] Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, 32 Georgia Inst. Tech. Scheller College of Bus. Res. Paper No. 36, at 8 (Dec. 18, 2015), http://ssrn.com/abstract=2709619. 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."

[2] For discussion of the history, *see* Peter 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.

[3] *See id.* at 1323: "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 counterespionage, nations that are friends in some respects may be acting contrary to U.S. 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."

[4] *Id.* at 1365.

[5] The materials that have been declassified contain redacted material, to protect national security-sensitive information. These redactions also play a privacy protective role, by preventing public release of the identities of individuals whose information was collected in a foreign intelligence investigation.

I. *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 of 2015.[6] The section closes by showing the FISC's willingness to exercise its constitutional power to restrict surveillance that it believes is unlawful.

II. *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 interlocking 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 (1) the National Security Agency (NSA) electing to terminate an Internet metadata collection program; (2) substantial privacy-enhancing modifications to the Upstream program; (3) the deletion of all data collected via Upstream prior to October 2011; and (4) a temporary prohibition on the NSA accessing one of its own databases.

III. *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 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.

IV. *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,

[6] The first statistics available are for the final months of 2015, when the USA FREEDOM Act had gone into effect. During this six-month period, the number of surveillance applications or certifications the FISC modified or rejected grew to 17 percent. *See* Section I(B)(4), *infra*, for a more detailed discussion.

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 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.

I. The FISC Exercises Independent and Effective Oversight over Surveillance Applications

[5] The FISC has been criticized in some media outlets as a "rubber stamp," particularly in the wake of the Snowden disclosures. This section shows how recently-declassified materials are not consistent with that claim. In my view, the FISC exercises effective oversight, backed by constitutional authority, over government applications to conduct surveillance.

[6] When it was founded in 1978, the FISC's primary task was to grant individual wiretap authorizations – such as for a single person suspected of acting as a Soviet agent. To evaluate government applications to conduct such wiretaps, the FISC applied FISA's probable cause standard to case-specific facts. Beginning in 2001, the FISC began to play an expanded role in overseeing entire surveillance programs. This role at times required the FISC to venture beyond a case-specific factual analysis and address new or significant legal and technical questions.

[7] This section provides an overview of the FISC's constitutional and statutory review powers, as well as illustrations of how the FISC has exercised those powers to evaluate proposed surveillance. Part A provides an overview of FISA and FISC rules for surveillance applications, as well as the FISC's application-review procedures, which can take surveillance applications through successive rounds of briefing, questioning, and hearings. Part B uses declassified FISC materials to show how the FISC has used its review powers in practice to oversee government surveillance. Part C uses an illustrative FISC case to show the constitutional authority the FISC is able to exercise when it believes surveillance runs afoul of the law.

A. FISC Procedural Rules and Review Procedures Ensure Thorough Oversight of Government Surveillance

[8] FISA and the FISC's procedural rules set content standards for government surveillance applications, and provide the FISC with a number of avenues with which to investigate proposed surveillance. Additionally, the FISC has established review procedures that generally subject surveillance applications to successive rounds of review.

1. FISA and FISC Rules of Procedure Require Detailed Surveillance Applications

a. *FISA Requirements for Surveillance Applications*

[9] FISA requires government agencies to submit detailed surveillance applications to the FISC. Government applications contain information that allows the FISC to understand what the government wants to do, as well as legal or constitutional implications the proposed surveillance presents.

[10] A traditional FISA application to surveil the communications of an individual person contains, at the least, the following:

(1) the identity of the government attorney making the application;[7]
(2) the identity of the individual to be targeted, if known;[8]
(3) a statement from a federal officer setting forth the facts purportedly justifying surveillance of the individual's communications;[9]
(4) a description of how – and how long – the government proposes to conduct the surveillance;[10]
(5) minimization measures, *i.e.* the government's proposed methods for minimizing the privacy impact of the surveillance on non-targeted persons;[11]
(6) a certification from a senior intelligence official, such as the Director of National Intelligence, describing the information sought; certifying that it constitutes foreign intelligence information; and stating that the information cannot be obtained by "normal investigative techniques;"[12] and
(7) an approval by a senior official in the Department of Justice, such as the Attorney General, stating that the application satisfies the requirements of FISA.[13]

[11] For larger programs such as those under Section 702, the US Attorney General and the Office of the Director of National Intelligence must jointly submit (1) "targeting procedures," *i.e.* procedures for ensuring that persons targeted for surveillance are foreign nationals located outside of the US; and (2) "minimization procedures," *i.e.* procedures for minimizing the impact that surveillance has on individuals' privacy.[14]

---

[7] *See* 50 U.S.C. § 1804(a)(1).
[8] *Id.* § 1804(a)(2).
[9] *Id.* § 1804(a)(3).
[10] *Id.* § 1804(a)(7), (9).
[11] *Id.* § 1804(a)(4).
[12] *Id.* § 1804(a)(6).
[13] *Id.* § 1804(a); 1805(a). The Department of Justice approval of a FISA application may be signed by the acting Attorney General, the Deputy Attorney General, or the Assistant Attorney General for National Security.
[14] *See* 50 U.S.C. § 1881a. For a more detailed discussion of Targeting and Minimization Procedures, *see* Chapter 3, Section III(C). Section 702 certifications also contain affidavits submitted by the directors of intelligence agencies, *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statement by the Office of the Director of National Intelligence and the Department of Justice on the Declassification of Documents Related to Section 702 of the Foreign Intelligence Surveillance Act*, IC ON THE RECORD (Sept. 29, 2015),

[12] As a result, surveillance applications presented to the FISC must receive multiple levels of signatures, including from senior officials. Based on my experience and discussions with officials in these agencies, it takes considerable work to get these signatures for applications and certifications. The amount of such work serves as a significant deterrent to seeking a FISA order except for high-value investigations.

b. *Additional Notice and Briefing Requirements under the FISC Rules of Procedure*

[13] The FISC's Rules of Procedure[15] are designed to ensure that the FISC receives notice of significant issues, as well as the briefing on those issues. If a surveillance application involves "an issue not previously presented" to the FISC – such as "a novel issue of law" or new technology – the government's application must inform the FISC about the nature and significance of the issue.[16] Similarly, whenever the government intends to use a "new surveillance or search technique," the government must submit briefing that:

(1) explains the technique;
(2) describes the circumstances in which it will be used;
(3) addresses any legal issues the technique raises; and
(4) states how the government will minimize the technique's impacts on fundamental rights.[17]

[14] Comparable briefing requirements apply when the government seeks to use an existing surveillance technique in a new way.[18] Lastly, whenever a surveillance application raises a novel issue of law, the government must submit a legal brief – either prior to or as part of its application – addressing the issue.[19]

2. Standard FISC Procedures Secure Multiple Rounds of Review of Surveillance Applications

[15] Since its establishment in 1978, the FISC has developed regular procedures for reviewing surveillance applications. Recently-published materials provide insight into how the FISC

---

https://icontherecord.tumblr.com/post/130138039058/statement-by-the-office-of-the-director-of (showing affidavits submitted by the Director of the FBI, the Director of the NSA, and the Director of the CIA in connection with 2014 Section 702 certification).

[15] The FISC has made its Rules of Procedure publicly available on its website. *See* F.I.S.C. R.P., http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

[16] F.I.S.C. R.P. 11(a). The FISC indicates that in programs authorized under Section 702, briefing on new issues is regularly included in certifications requesting reauthorization: "The government's submission of a Section 702 application typically includes a cover filing that highlights any special issues and identifies any changes that have been made relative to the prior application." *See* Letter dated July 29, 2013 from Reggie B. Walton, FISC Chief Judge, to Patrick J. Leahy, Chairman of the US Senate Judiciary Committee 2 [hereinafter "Chief Judge Walton Letter"], http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Grassley-1.pdf.

[17] F.I.S.C. R.P. 11(b).

[18] *Id.* 11(c).

[19] *Id.* 11(d).

applies these procedures in practice.[20] This section summarizes the more salient aspects of the FISC review process that a government surveillance application goes through to be approved, modified, or rejected by the FISC.

a. *Initial Review, Follow-Up, and Written Analysis by Security-Cleared Staff Attorneys*

[16] The FISC is supported by a full-time staff of security-cleared attorneys employed by the Judicial Branch (not subject to review by the NSA or any other agency). When a government agency files an application to conduct surveillance, one of the FISC's staff attorneys receives the application and conducts an initial review as to whether the application satisfies statutory and constitutional requirements.[21] For larger submissions – such as the yearly certifications to reauthorize programs under Section 702 – a team of staff attorneys can share responsibility for initial review.[22]

[17] As part of his or her review, the staff attorney will often engage in telephone conversations with the government agency to raise concerns, seek additional information, or ask for clarification.[23] The attorney then prepares a written analysis of the application for the FISC judge responsible for the matter. This analysis sets forth any concerns about the legality of the government's proposed surveillance, and may identify areas where further information is necessary or modifications are recommended.[24]

b. *Review by FISC Judges, and Ongoing Review through Further Proceedings*

[18] After the FISC's staff attorneys have completed their initial review, a FISC judge reviews the surveillance application as well as the staff attorney's written analysis. The FISC Rules of Procedure provide the FISC judge with multiple avenues to proceed:

---

[20] This section generally refers to procedures developed for FISC review of applications for individual FISA wiretap warrants. Where differences in procedures exist for review of larger certifications relating to surveillance programs, this section notes the difference. The FISC's powers to evaluate proposed surveillance, such as posing questions, requiring follow-up meetings, and holding hearings, do not change depending on the type of application or certification it is examining.

[21] *See* Chief Judge Walton Letter, *supra* note 16, at 2. The submission presented to the FISC at this point in review proceedings is not a "final" application; it is commonly referred to as a "read copy," *i.e.* a near-final version of the application that does not yet have the required agency signatures. The difference between "read-copy" and "final" applications is discussed in Section I(A)(2)(c), *infra*.

[22] *Id.* at 4.

[23] *Id.* at 2. The FISC indicates that its staff attorneys are on the phone with the government "every day" in connection with reviews of surveillance applications. *See id.* at 2-3.

[24] *Id.* ("A Court attorney [] prepares a written analysis of the application for the duty judge, which includes an identification of any weaknesses, flaws, or other concerns. For example, the attorney may recommend that the judge consider requiring the addition of information to the application; imposing special reporting requirements; or shortening the requested duration of an authorization.") (internal citation omitted).

- The FISC can order the government "to furnish any information that [the FISC] deems necessary."[25]

- The FISC can exercise any "authority . . . as is consistent with Article III of the [US] Constitution," which includes posing follow-up questions to the government, or ordering the government to provide additional briefing on legal, technical, or factual issues.[26]

- FISC judges can direct the agency seeking surveillance to meet with FISC staff attorneys, in person or via telephone, to discuss concerns or clarify issues.[27]

- The FISC can order hearings, compel government representatives to appear, and compel government representatives to testify under oath or provide other evidence.[28] When the FISC orders a hearing, government officials who provided factual information in a surveillance application by rule "must attend the hearing" – along with any further representatives the FISC directs.[29] The FISC indicates that, at a minimum, its hearings are attended by the agency attorney who prepared the surveillance application at issue, as well as a fact witness from the agency seeking surveillance.[30]

[19] As discussed below, the FISC has made use of these powers in the course of its evaluation of surveillance applications and certifications.

c. *FISC Indication of Disposition Can Result in Voluntary Modification to Applications*

[20] The FISC's review proceedings can result in an iterative process where the government responds to FISC-identified issues, offering the government opportunities to cure deficiencies in surveillance applications as review is ongoing. Generally speaking, the government will submit a preliminary surveillance application, which will undergo the successive review steps described above and any further steps the FISC deems necessary, such as a hearing.[31] After the FISC has satisfied itself that it understands the government's proposed surveillance as well as its legal implications, the FISC will indicate to the government the manner in which it intends to dispose of the application – *e.g.* by granting it, modifying it, or rejecting it.[32]

---

[25] F.I.S.C. R.P. 5(c).
[26] *Id.* 5(a).
[27] *See* Chief Judge Walton Letter, *supra* note 16, at 6.
[28] F.I.S.C. R.P. 17(a), (d).
[29] *Id.* 17(c).
[30] Chief Judge Walton Letter, *supra* note 16, at 6.
[31] The FISC has referred to the preliminary application as a "read copy," which is a "near-final version of the government's application" that does not yet include the required signatures of executive branch officials. *Id.* at 2 n.2.
[32] *See id.* at 3: "Th[e] courses of action [available to the FISC] might include indicating to Court staff that he or she is prepared to approve the application without a hearing; indicating an inclination to impose conditions on the

[21] After the FISC indicates its intended disposition, the government must determine the course of action it deems best, such as voluntarily amending its application, withdrawing the application, providing additional information, or moving forward while asking the FISC to reconsider its position – or a combination thereof. When the government decides to move forward with its application, it submits a "final" application to the FISC for a ruling.[33] My understanding is that only these "final" applications are included in the statistics publicly released each year.[34] Consequently, applications that are not made final, or that need modification before they become final, do not traditionally appear in the annual statistics, although the USA FREEDOM Act has introduced reporting provisions that have resulted in statistics reflecting these details for the latter part of 2015.[35] This weeding-out process before the applications become "final" thus can lead to a misleading conclusion that all or almost all applications are approved by the Court. Instead, the standards insisted on by the FISC for a "final" application mean that the agency lawyers must meet those standards before undertaking the bureaucratic effort to get signatures from senior officials.[36]

---

approval of the application; determining that additional information is needed about the application; or determining that a hearing would be appropriate before deciding whether to grant the application."

[33] *Id.* The government may also request a hearing in conjunction with its submission of a final application, even if the FISC has not yet required one.

[34] FISC statistics have traditionally been provided in reports the Department of Justice submits to Congressional oversight committees pursuant to FISA provisions that require reports on "the total number of applications made for [FISC] orders" and "the total number of such orders . . . either granted, modified, or denied." *See* 50 U.S.C. § 1807. The USA FREEDOM Act now requires the Administrative Office of the US Courts (which is housed within the Judicial Branch) to compile and provide statistics on the applications presented to the FISC for approval. *See* 50 U.S.C. § 1873(a). These statistics are discussed in detail in Section I(B)(4), *infra*.

[35] The FISC addressed this issue in the Chief Judge Walton, *supra* note 6, to the US Senate Judiciary Committee:

> The annual statistics provided to Congress by the [Department of Justice] [] – frequently cited to in press reports as a suggestion that the Court's approval rate of applications is over 99% – reflect only the number of *final* applications submitted to and acted on by the Court. These statistics do not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them.

Chief Judge Walton Letter, *supra* note 16, at 3 (emphasis in original). Section I(B)(4), *infra*, addresses how the Judicial Branch has recently begun to publish statistics reflecting the number of surveillance applications the government voluntarily modifies during FISC review proceedings.

[36] For example, when the FISC itself tracked the number of applications that were substantially altered in response to concerns raised during the review processes – as opposed to only final applications that were denied or modified via formal order – the statistics showed significantly more intervention than the traditional statistics reported by the Department of Justice:

> During the three month period beginning from July 1, 2013 through September 30, 2013, we have observed that 24.4% of matters submitted ultimately involved substantive changes to the information provided by the government or to the authorities granted as a result of Court inquiry or action.

Chief Judge Walton Letter, *supra* note 6, at 1.

[22] The FISC resolves the final application via an order, which can be accompanied by a memorandum opinion explaining the Court's legal reasoning. To the extent surveillance is granted, the terms of the FISC's order govern what the government may and may not do.

B. The FISC Is Not a "Rubber Stamp," but Instead Thoroughly Scrutinizes Government Surveillance Applications

[23] As I mentioned above, particularly following the Snowden disclosures, the FISC was criticized as a "rubber stamp." This can be understood as a criticism that, while the FISC may have substantial review powers, it does not use them in practice. Until recently, there were few publically-available FISC materials that permitted this criticism to be evaluated. Now, many of the recently-declassified materials provide insight as to how the FISC has exercised its review authority to oversee government surveillance applications.

[24] My review of the declassified materials supports the conclusion that the FISC exercises thorough review of surveillance applications. Of course, the procedures the FISC orders in a particular case are influenced by "the nature and complexity of [the] matte[r] pending before the Court."[37] This section will consider example FISC cases to illustrate various ways in which the FISC has scrutinized proposed surveillance: (1) the FISC uses its review powers to require successive rounds of briefing, questioning, and hearings; (2) the FISC gains the technical knowledge necessary to understand the implications of proposed surveillance; (3) the FISC focuses on government compliance when determining whether it should permit surveillance; (4) the FISC modified a significant number of recent surveillance applications; and (5) the FISC has proactively required the government to justify surveillance techniques the FISC anticipates arising in future cases.

1. The FISC Uses its Article III Powers to Ensure Thorough Review

[25] The FISC has made use of its Article III powers to engage in, and to require the government to respond to, successive rounds of review investigating the government's proposed surveillance. The FISC can pose questions in response to surveillance applications, direct government agencies to meet with FISC staff attorneys, order further briefing, and hold hearings to resolve technical or legal questions.

[26] An illustration of how the FISC has exercised these review powers in a more complex case can be seen in a 2008 opinion in which the FISC authorized Section 702 programs.[38] To conduct these programs, the government is required to obtain FISC approval of targeting and minimization procedures it proposes to govern its selection of intelligence targets and its collection of communications. To evaluate what the government's proposed procedures entailed, and to evaluate the legality of the government's desired surveillance, the FISC employed the following review procedures:

---

[37] *Id.* at 6.

[38] *In re DNI/AG Certification [Redacted]*, No. 702(i)-08-01 (F.I.S.C. Sept. 4, 2008), https://www.dni.gov/files/documents/0315/FISC%20Opinion%20September%204%202008.pdf.

- The FISC conducted a preliminary review of the certification's legality.[39]
- The FISC directed the government to meet with FISC attorneys. FISC staff attorneys "met with counsel for the government to communicate the Court's questions regarding the proposed targeting and minimization procedures."[40]
- After the meeting, the government submitted preliminary responses to the questions the FISC had posed.[41]
- The FISC then held a hearing "during which the government answered additional questions and provided additional information."[42]
- Following the hearing, the government made two supplemental submissions to the FISC.[43]
- The government also submitted internal guidelines created by the US Attorney General and Director of National Intelligence designed to ensure compliance with the certification submitted to the court.[44]
- The FISC issued a 42-page written opinion evaluating the legality and constitutionality of the government's proposed surveillance.[45]

[27] The above reflects the review process available for any surveillance application or certification presented to the FISC. Declassified materials show the FISC subjecting other Section 702 certifications to similarly careful review, at times involving up to five rounds of government briefing,[46] discussions with staff attorneys and hearings,[47] and an 80-page opinion evaluating legal aspects of the government's certification.[48] As can be seen from further case summaries in this Chapter, the FISC is willing to exercise its review powers in cases presenting significant issues.

2. The FISC Develops the Technical Understanding Necessary to Adjudicate Surveillance Applications

[28] Many surveillance oversight bodies, whether in the US or elsewhere, have at some point been criticized as lacking the technical knowledge necessary to assess surveillance technology.[49]

---

[39] *Id.* at 5.
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.* at 5-6.
[45] *Id.* at 33-41.
[46] *See [Caption Redacted]*, No. [Redacted], 2011 WL 10945618 (F.I.S.C. Oct. 3, 2011), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.
[47] *See [Caption Redacted]*, No. [Redacted] (F.I.S.C. Aug. 26, 2014), https://www.aclu.org/sites/default/files/field_document/fisc_opinion_and_order_re_702_dated_26_august_2014_ocrd.pdf.
[48] *See [Caption Redacted]*, No. [Redacted] (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[49] For example, the German press has alleged that Germany's G-10 Commission, which is responsible for approving governmental surveillance applications, lacks the technical knowledge to adequately police German surveillance agencies such as the *Bundesnachrichtendienst* (BND). *See* Kai Biermann, *BND-Kontrolleure verstehen nichts von Überwachungstechnik [BND Overseers Understand Nothing about Surveillance Technology]*, DIE ZEIT (Oct. 7, 2013), http://www.zeit.de/digital/datenschutz/2013-10/bnd-internet-ueberwachung-provider.

The FISC's rules and procedures permit it to close gaps in technical understanding, and to focus on the implications of the technology that government agencies are seeking permission to use. As stated above, FISC rules require the government to bring any new techniques or technology it intends to use to the FISC's attention, and to brief both the technical aspects as well as legal implications of new technology.[50] Additionally, FISC judges can order further briefing, ask questions, and hold hearings.[51] FISC judges' service in US federal district courts provides them with experience in clarifying complex issues.

[29] The FISC's ability to engage in technical analysis is illustrated by an exchange between the FISC and the NSA that took place in the summer of 2011. At that time, the NSA informed the FISC that some of its content-acquisition systems were collecting data packets known as "Internet transactions," as opposed to discrete communications such as single emails.[52] Internet transactions could contain a single email, but they could also contain multiple communications from different senders to different recipients.

[30] The FISC wanted to clarify the nature of Internet transactions, as well as the legal implications of collecting transactions instead of communications. The following events reflect the orders the FISC issued in this regard, as well as the government's responses to them:

- On May 9, 2011, the FISC "directed the government to answer a number of questions in writing;"[53]
- On June 1, 2011, the government submitted written answers;[54]
- On June 17, 2011, the FISC "directed the government to answer a number of follow-up questions;"[55]
- On June 28, 2011, the government submitted written answers to the FISC's follow-up questions;[56]
- On July 8, 2011, the FISC met with senior DOJ officials to discuss the government's answers to its questions. During the meeting, the FISC expressed "serious concerns regarding NSA's acquisition of Internet transactions;"[57]
- On August 16, 2011, the government submitted a "statistically representative sample of the nature and scope of the Internet communications acquired through" the Upstream program;[58]
- On August 22, 2011, FISC staff attorneys met with DOJ representatives;[59]

---

[50] *See* F.I.S.C. R.P. 11(b): "Prior to requesting authorization to use a new surveillance or search technique, the government must submit a memorandum to the Court that: (1) explains the technique; (2) describes the circumstances of the likely implementation of the technique; (3) discusses any legal issues apparently raised; and (4) describes the proposed minimization procedures to be applied."
[51] *See id.* at 5, 17.
[52] *See [Caption Redacted]*, No. [Redacted], 2011 WL 10945618, https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.
[53] *Id.* at 7.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.* at 8.
[58] *Id.* at 9.

- On August 30, 2011, the government submitted further briefing for FISC review;[60]
- On September 7, 2011, the FISC held a hearing "to ask additional questions of NSA and the [DOJ] regarding the government's statistical analysis and the implications of that analysis;"[61]
- On September 9, 2011, the government made an additional written submission to the FISC;[62]
- On September 13, 2011, the government made its final written submission to the FISC.[63]

[31] Through this process, the FISC had the opportunity to develop a technical understanding of Internet transactions, as well as briefings, meetings, and a hearing to evaluate the legal implications of transaction-based collection. The FISC then issued three orders covering over 100 pages describing Internet transactions and the legal consequences of transaction-based collection for the NSA.[64] These review powers are available to the FISC in any matter that raises novel technical issues.

3. The FISC Focuses on Compliance when Evaluating Governmental Surveillance Applications

[32] Compliance with prior FISC orders is a significant factor in FISC decisions to authorize, modify, or deny surveillance applications and certifications. When the government asks the FISC for permission to conduct surveillance, the FISC may review the government's past compliance with similar orders – or ongoing compliance with existing orders – in deciding whether to authorize the government's proposed surveillance. This is particularly true for longer-running programs such as PRISM, where compliance incident reporting (which will be discussed in more detail in section II.A. below) provides feedback for the FISC to judge how its orders are being implemented.

[33] The General Counsel of the Office of the Director of National Intelligence describes the FISC's focus on compliance when evaluating Section 702 certifications as follows:

> The FISC carefully reviews the targeting and minimization procedures for compliance with the requirements of both the statute and the [US Constitution]. The FISC does not, however, confine its review to these documents. [The] FISC receives extensive reporting from the [g]overnment regarding the operation of, and any compliance incidents involved in, the Section 702 program. . . . The FISC considers . . . the [g]overnment's compliance annually when it evaluates

---

[59] *Id.* at 9.
[60] *Id.*
[61] *Id.* at 9-10.
[62] *Id.* at 10.
[63] *Id.*
[64] *See id.*; *see also [Caption Redacted]*, No. [Redacted], 2011 WL 10947772 (F.I.S.C. Nov. 30, 2011), http://www.fas.org/irp/agency/doj/fisa/fisc1111.pdf; *[Caption Redacted]*, No. [Redacted] (F.I.S.C. Sept. 25, 2012), https://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.

> whether a proposed certification meets all statutory and Constitutional requirements.[65]

[34] Similarly, the Privacy and Civil Liberties Oversight Board – after reviewing NSA compliance and FISC practice – summarized the role of compliance reports for the FISC's review of Section 702 certifications as follows:

> [C]ompliance notices must state both the type of noncompliance that has occurred and the facts and circumstances relevant to the incident. In doing so, representations to the [FISC] have in essence created a series of precedents regarding how the government is interpreting various provisions of its targeting and minimization procedures, which informs the court's conclusions regarding whether those procedures – as actually applied by the Intelligence Community to particular, real-life factual scenarios – comply with [statutory requirements and the Constitution].[66]

[35] A recently-declassified FISC opinion illustrates how the FISC has evaluated NSA compliance when determining whether to authorize surveillance programs. In July 2014, the NSA submitted a certification asking the FISC to reauthorize Section 702 programs. In evaluating the NSA's certification, the FISC began from the position that its review "is not confined to [NSA-proposed targeting and minimization] procedures as written; rather, the Court also examines how the procedures have been and will be implemented."[67] In other words, the FISC "examines the government's implementation of, *and compliance with*," the government's proposed targeting and minimization procedures to determine whether to approve them.[68] The FISC noted that it had "examined quarterly compliance reports submitted by the government," as well as "individual notices of non-compliance relating to implementation of Section 702."[69] Based on this review, the FISC had directed its staff attorneys to convey "a number of compliance-related questions to the government," to which the government responded in writing.[70] The FISC then held a hearing regarding changes to targeting and minimization procedures, as well as "certain compliance matters."[71]

[36] The FISC ultimately determined that the Section 702 programs should be reauthorized, but also required the NSA to submit additional reports on its implementation of certain

---

[65] *Joint Unclassified Statement to the H. Comm. on the Judiciary*, 114th Cong. 4 (2016) [hereinafter *Joint Statement*] (statement of Robert Litt, General Counsel of the Office of the Dir. of Nat'l Intelligence, et al.), https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2016/02/17/508_compliant_02-02-16_fbi_litt_evans_steinbach_darby_joint_testimony_from_february_2_2016_hearing_re_fisa_amendments_act.pdf.

[66] PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 35, https://www.pclob.gov/library/702-Report.pdf [hereinafter PCLOB 702 REPORT].

[67] *[Caption Redacted]*, No. [Redacted] at 3 (F.I.S.C. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

[68] *Id.* at 26 (emphasis added).

[69] *Id.* at 3.

[70] *Id.*

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

compliance standards.[72] Within the FISC's 43-page opinion evaluating the case for reauthorization, the court evaluated intelligence agencies' measures for ensuring compliance with FISA and FISC orders.[73]

[37] One year later in summer 2015, the Department of Justice presented the next certification to reauthorize Section 702 programs.[74] The FISC reiterated that its review of the certification required examining how NSA targeting and minimization procedures "have been and will be implemented."[75] The FISC then "examined quarterly compliance reports submitted by the government since the most recent FISC review of Section 702," as well as "individual notices of non-compliance."[76] Based on this review, the FISC directed its staff attorneys to convey "a number of compliance-related questions to the government."[77] Afterwards, the FISC "conducted a hearing to address some of the same compliance-related questions."[78] The FISC ultimately reauthorized the Section 702 programs, but imposed further reporting requirements and scheduled a follow-up hearing to monitor compliance.[79]

4. The FISC Modified a Significant Percentage of Surveillance Applications

[38] For many years, one of the FISC's important functions was to insist that surveillance agencies and the Department of Justice clearly document surveillance requests. I discussed this role of the FISC in 2004, stating that FISA purposefully made assembling surveillance applications burdensome so that the FISC had structural assurances the government was seeking true foreign-intelligence information via proposed surveillance.[80] The effect was that agencies would only go through the effort of obtaining the FISC's approval for high-priority surveillance requests. In recent decades, as the threat landscape has changed, the number of surveillance applications presented to the FISC has increased significantly.

[39] As outlined above, the FISC's standard review procedures provide multiple opportunities for the FISC to express concerns about proposed surveillance, and for the government to address FISC-identified deficiencies as review is ongoing. Despite this, the FISC substantially modified a significant number of recent surveillance applications. The USA FREEDOM Act introduced new statutory provisions requiring the Judicial Branch to report statistics on applications and

---

[72] *Id.* at 40-42.
[73] *See id.* at 7-13.
[74] *See [Caption Redacted]*, No. [redacted] (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[75] *Id.* at 7.
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *See id.* at 78.
[80] *See* Swire, *supra* note 2, at 1327: "All those signatures served a purpose, to assure the federal judge sitting in the FISA court that a national security wiretap was being sought for 'intelligence purposes' and for no other reason—not to discredit political enemies of the White House, not to obtain evidence for a criminal case through the back door of a FISA counterintelligence inquiry." (quoting JIM MCGEE & BRIAN DUFFY, MAIN JUSTICE 318 (1996)).

certifications presented to the FISC for approval,[81] and the Judicial Branch's statistics now reflect the number of recent proposed orders the government voluntarily modified during FISC review proceedings.[82] From June 8, 2015 to December 31, 2015, the FISC received approximately 1,010 surveillance applications.[83] The FISC rejected five of these applications, and substantially modified 169.[84] As a result, the FISC either rejected or modified just over 17% of all surveillance applications it received in the latter half of 2015.[85]

[40] These statistics bolster claims that the FISC attentively scrutinizes governmental surveillance applications. Nonetheless, criticism persists that the FISC should not be considered an effective oversight body because it rarely completely rejects entire government surveillance applications. While I respect the privacy concerns behind this criticism, I believe it does not account for the full picture of how the FISC can resolve concerns regarding proposed surveillance. Four reasons help explain why FISC practice rarely results in full rejection of an application:

---

[81] *See* 50 U.S.C. § 1873(a): The Director of the Administrative Office of the United States Courts shall annually submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, subject to a declassification review by the Attorney General and the Director of National Intelligence, a report that includes:

(A) the number of applications or certifications for orders submitted under each of sections 1805, 1824, 1842, 1861, 1881a, 1881b, and 1881c of this title;
(B) the number of such orders granted under each of those sections;
(C) the number of orders modified under each of those sections;
(D) the number of applications or certifications denied under each of those sections;
(E) the number of appointments of an individual to serve as amicus curiae under section 1803 of this title, including the name of each individual appointed to serve as amicus curiae; and
(F) the number of findings issued under section 1803(i) of this title that such appointment is not appropriate and the text of any such findings.

[82] *SEE* REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE US COURTS ON ACTIVITIES OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS FOR 2015 3, http://www.uscourts.gov/statistics-reports/analysis-reports/directors-report-foreign-intelligence-surveillance-courts [hereinafter "REPORT ON THE ACTIVITIES OF FISC"]. The Report defines the "Orders Modified" category so it now includes modifications to proposed orders that "resulted from the [FISC]'s assessment of" an application or certification, including when the as-modified proposed orders "were subsequently reflected in . . . a signed, final application or certification." *See id.* at 2.

[83] *See id.* at 3.

[84] *Id.* The statistics are higher than in the past because the latter half of 2015 is the first period in which there was reporting on the number of proposed orders the government altered in response to FISC-identified concerns, as opposed to reporting only the number of final applications the FISC rejected or modified via formal order. In contrast, the Department of Justice's more traditional 2015 FISC statistics stated that they only captured modifications to "*final* application[s]." When only modifications to final applications were counted, the statistics showed a five percent modification rate, although the FISC substantially modified a total of 80 final applications. *See* DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GEN., Letters dated Apr. 28, 2016 from Peter J. Kadzik, Assistant Attorney Gen. regarding Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2015 1-2 (2016), https://www.justice.gov/nsd/nsd-foia-library/2015fisa/download.

[85] Some modifications the government voluntarily made to surveillance applications in response to FISC-identified concerns are not reflected in these statistics. The modification statistics reflect changes the government voluntarily made to proposed surveillance *orders* in response to FISC concerns, but do not reflect changes the government voluntarily made to surveillance *applications* (or the certifications supporting them). *See* REPORT ON THE ACTIVITIES OF FISC, *supra* note 82, at 2-3.

First, the FISC rarely rejects surveillance applications because its review process often avoids the need for rejection. Concerns that would otherwise lead to rejection can be identified through meetings with the FISC's staff attorneys, FISC hearings, or further briefing ordered by the FISC. FISC proceedings thus permit the government to correct legal and technical issues during the review phase, subject to the FISC's subsequent approval.

Second, surveillance application practice before the FISC has developed over the course of decades. Many applications involve a combination of elements that have been in use for significant time after FISC review, as well as newer elements. Such requests need not be rejected outright, but instead modified where necessary.

Third, the FISC can require agencies to report on how they conduct surveillance in practice, instead of rejecting measures without data as to how they operate. For example, in a recent opinion, the NSA's proposed minimization measures permitted the NSA to disseminate data in response to legal "mandates."[86] The FISC expressed concern that this provision could undermine privacy protections, but the NSA stated it would follow a narrow interpretation. The FISC (1) stated it would only permit legal provisions that "clearly and specifically requir[e] action" to justify dissemination under this provision, and (2) required the NSA to "promptly" report any dissemination of data made in response to a legal mandate.[87] Each NSA report had to "identify the specific [legal] mandate" the NSA claimed justified the dissemination.[88]

Fourth, by the time they reach the FISC, FISA applications have already undergone layers of review (thus reducing the chance that any individual application will be rejected). A surveillance application must be signed by high-level officials from both the Department of Justice (such as the Attorney General) and the intelligence community (such as the Director of National Intelligence).[89] Review by Department of Justice lawyers helps ensure that technical defects that could lead to rejection are cured. FISA's dual-signature requirements also ensures that at least two agencies – one of which is the Department of Justice – as well as senior officials have determined that proposed surveillance is important enough to be presented to the FISC, and that the surveillance application is FISC-worthy.[90]

[41] Despite these structured hurdles, Judicial Branch statistics show the FISC either rejected or substantially modified 17 percent of all the applications and certifications presented to it during the latter half of 2015. This statistic is higher than in previous reporting periods, but it indicates practice in the wake of the changes since 2013 and shows current evidence that the

---

[86] *See [Caption Redacted]*, [Case no. redacted] (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[87] *Id.* at 23, 78.
[88] *Id.* at 78.
[89] *See* 50 U.S.C. § 1804.
[90] For my discussion of how the FISA signature requirements were designed to signal the legitimacy of proposed intelligence to the FISC, *see* Swire, *supra* note 2, at 1327.

FISC is willing to intervene to conform proposed surveillance to legal and constitutional requirements.

5. The FISC Proactively Requires the Government to Justify Surveillance Techniques it Believes Will Raise Privacy Issues in Future Applications

[42] One lesser-known fact about the FISC is that its eleven judges meet for semi-annual conferences.[91] At these conferences, FISC judges can raise concerns about surveillance practices they anticipate arising in future cases. As a result of these discussions, the FISC may exercise its statutory or constitutional powers on its own motion to require the government to justify its use of particular surveillance techniques.

[43] A recently declassified FISC opinion illustrates the proactive oversight that can result from the FISC's internal discussions.[92] The opinion reflects how the FISC required the government to justify capturing information known as "post-cut-through digits." As background, FISA permits the FISC to approve surveillance via Pen Register/Trap-and-Trace (PR/TT) devices. PR/TT devices capture information about calls transmitted by, or received by, a particular telephone. Under FISA, PR/TT surveillance is permitted to obtain telephony metadata (such as numbers dialed, date, and time), but it may not be used to obtain "the contents of any communication."[93] "Post-cut-through digits" refer to digits entered by a caller after a phone call has been placed (or "cut through"). They can represent part of dialing information – for example, if a caller is using an international calling card and must enter the destination number after connecting with the card service – in which case they are metadata. They can also represent content, such as when a caller dials his bank's automated service and enters prompts to perform a transfer. Existing PR/TT technology is not able to distinguish between the two types of post-cut-through digits. The FISC had required the government to brief the lawfulness of acquiring post-cut-through digits on previous occasions.

[44] In October 2015, the FISC judges met for a semi-annual conference. There, "the FISC judges discussed the issues presented by post-cut-through digits."[94] After some FISC judges expressed "concerns," "it was the consensus of the judges that further briefing was warranted."[95] Two days after the conference, the FISC ordered the government to submit briefing addressing "the lawfulness of acquiring post-cut-through digits under PR/TT orders."[96]

---

[91] For a reference to FISC judges' semi-annual conferences, *see In [Redacted] a U.S. Person*, No. PR/TT 2016-[Redacted] at 5 (F.I.S.C. Feb. 12, 2016), https://www.dni.gov/files/icotr/PCTD%20FISC-R%20Certification%2020160818%20pdf.pdf.

[92] *See id.*

[93] *See* 18 U.S.C. § 3127(3) (excluding "the contents of any communication" from information that may be obtained via pen registers); *id.* § 3127(4) (excluding "the contents of any communication" from information that may be obtained via trap-and-trace devices).

[94] *In [Redacted] a U.S. Person*, No. PR/TT 2016-[Redacted] at 5 (F.I.S.C. Feb. 12, 2016), https://www.dni.gov/files/icotr/PCTD%20FISC-R%20Certification%2020160818%20pdf.pdf.

[95] *Id.*

[96] *Id.*

[45] As a result of the FISC's order, the government submitted briefing, and the FISC issued an opinion reviewing existing authorities and authorizing the capture of post-cut-through digits via PR/TT surveillance.[97] The FISC then certified its decision for appeal to the Foreign Intelligence Surveillance Court of Review (FISCR), which reviews appeals from the FISC.[98] The FISCR appointed an *amicus curiae* to argue against the government, received adversarial briefing, and issued a 38-page opinion affirming the FISC's decision.[99] Thus, as a result of the FISC's discussions at its semi-annual conference, the issue of post-cut-through digits was revisited, subjected to two levels of review, and had the benefit of third-party briefing.

C. FISC Exercises Constitutional Authority in Overseeing Executive Branch Surveillance

[46] As I stated in Chapter 3, the FISC is a federal court established under Article III of the US Constitution. This means that the FISC may exercise the constitutional authority granted to the US Judicial Branch in investigating, modifying, or terminating surveillance that the FISC believes does not satisfy applicable statutes or the US Constitution.

[47] The FISC's constitutional power is perhaps best illustrated by the FISC's halting President Bush's so-called "warrantless wiretapping" program. Following the September 11 terror attacks, President Bush authorized the NSA – without informing the FISC – to acquire the communications of persons the NSA suspected of being associated with international terrorism. This program was titled "StellarWind." The warrantless wiretapping program eventually become public, as a significant program in my experience generally does sooner rather than later.[100] The NSA sought to bring it under FISC oversight, filing an application with the FISC requesting that the court approve StellarWind as it had existed to date.[101]

[48] Concretely, the NSA asked the FISC to authorize it to conduct "electronic surveillance of telephone numbers and email addresses thought to be used by international terrorists" – without a FISC judge first determining that the persons so targeted were suspected of international terrorism.[102] The NSA stated StellarWind was "necessary to provide . . . the speed and flexibility with which NSA responds to terrorist threats," and asserted that if the FISC refused to permit the program to continue, "vital foreign intelligence information may be lost."[103]

---

[97] The FISC found that no existing technology permitted the government to distinguish content from non-content post-cut-through digits, and that capturing such digits was reasonable under the Fourth Amendment. *See id.* at 6-13.
[98] *Id.* at 14. For a discussion of the FISCR and cases in which appeals lie, *see* Chapter 3, Section III(A).
[99] *See In re Certified Question of Law*, No. FISCR 16-01 (F.I.S.C.R. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf.
[100] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N. Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.
[101] *In re [Redacted]*, No. [Redacted] (F.I.S.C. Apr. 3, 2007), https://www.dni.gov/files/documents/1212/CERTIFIED%20COPY%20-%20Order%20and%20Memorandum%20Opinion%2004%2003%2007%2012-11%20Redacted.pdf.
[102] *Id.* at 18.
[103] *Id.* at 18-19.

[49] The FISC agreed that the prospect of losing vital intelligence was concerning, but denied the NSA's application.[104] The result was that either StellarWind had to end, or the surveillance laws had to change. The FISC ruled that FISA required a FISC judge to individually approve every telephone number or email address the NSA wished to target – regardless of whether the target was in the US or abroad. The Court acknowledged this would clearly burden the NSA's ability to surveil suspected terrorists, but held that it reflected the "balance struck by Congress between procedural safeguarding of privacy interests and the need to obtain intelligence information."[105] For the situation to change, the FISC stated Congress would need to "take note of the grave threats now presented by international terrorists," conclude that "FISA's current requirements are unduly burdensome," and construct new rules for "surveillances of phone numbers and e-mail addresses used overseas."[106] Until then, however, the FISC concluded it could not authorize StellarWind in its requested form.

[50] The FISC's ruling meant that a surveillance program authorized by the President could not continue in its present form. The FISC ultimately issued orders authorizing a modified form of the program, in which the FISC first approved the telephone numbers and email addresses used to conduct surveillance under this program.[107] After US agencies determined this modified version of the program was creating an "intelligence gap," Congress amended FISA by passing the Protect America Act (PAA) in 2007, followed by the FISA Amendments Act in 2008.[108]

[51] To me, the FISC's StellarWind decision represents careful judicial oversight of a major surveillance program. The FISC looked closely at NSA surveillance, found it may be useful and vital, but also determined that the existing laws did not permit it. The FISC therefore indicated its willingness to halt and modify the StellarWind program. In my view, this example illustrates the federal judges' attention to the rule of law. It was only after the Congress passed a new law authorizing the program under new rules, after public debate, that the FISC approved the program.

---

[104] Initially, the FISC permitted the program to continue for 30 days, during which time discussions between the FISC and the NSA regarding the program were ongoing. A different FISC judge then issued the opinion summarized here, which required the program to be modified. *See id.*

[105] *Id.* at 19.

[106] *Id.* at 19.

[107] The FISC initially extended the program by just under sixty days, during which period it permitted the government to draft and submit "a revised and supplemented application that would meet the requirements of FISA." *Id.* at 20-21. The FISC's modified orders, on the basis of FISA "roving" or "after-acquired" authorities, permitted the government to add some newly discovered telephone numbers and email addresses without an individual court order in advance. *See* Declassified Certification of Attorney General Michael B. Mukasey, at para. 38, *In re Nat'l Sec. Agency Telecommunications Records Litig*., MDL No. 06-1791-VRW (N.D. Cal. Sept. 19, 2008), http://www.dni.gov/files/documents/0505/AG%20Mukasey%202008%20Declassified%20Declaration.pdf; *see also* PCLOB 702 REPORT, *supra* note 66, at 17-18.

[108] *See* PCLOB 702 REPORT, *supra* note 66, at 18.

II. The FISC Monitors Compliance with its Orders, and Has Enforced with Significant Sanctions in Cases of Non-Compliance

[52] The FISC's jurisdiction is not limited to approving surveillance applications. The FISC also monitors government compliance and can enforce its orders.[109] When instances of noncompliance arise, the FISC has imposed significant sanctions. FISC compliance proceedings have resulted in substantial changes to, and termination of, NSA surveillance programs.

[53] This section outlines how the FISC monitors government compliance with its orders, and the measures the FISC is able to take when agencies fail to comply. Part A describes how the FISC receives notice of noncompliance. Part B then summarizes FISC decisions that illustrate how the FISC has responded to noncompliance, including the significant changes to NSA surveillance programs that have resulted. The conclusion discusses how the effectiveness of compliance oversight has evolved considerably since 2001.

A. The System of Compliance Incident Reporting

[54] The FISC uses compliance-incident reporting to monitor compliance with its orders. Interlocking reporting requirements, agency-internal oversight, third-party auditing, and periodic reporting exist to provide the FISC with notice of compliance incidents. This part will first outline the system of oversight and reporting structures within US executive agencies. It will then briefly sketch reporting requirements contained in FISC rules and orders.

1. Oversight and Reporting Structures within Executive Agencies

[55] Oversight, auditing, and reporting structures have been established across US executive agencies for the purpose of providing the FISC with timely notice of compliance incidents.

a. *The Department of Justice's Oversight Section*

[56] Compliance reporting is not placed exclusively in the hands of surveillance agencies such as the NSA. The Department of Justice is tasked with monitoring surveillance agencies' compliance with FISC orders and applicable laws, and reporting compliance incidents to the FISC. To accomplish its oversight mission, the Department maintains an Oversight Section within its National Security Division. The Oversight Section monitors US intelligence services; assesses agency implementation of FISA authorities; identifies and reports instances of noncompliance; and works with agencies to remediate compliance incidents.[110] The Department

---

[109] As an Article III court, the FISC has inherent authority to monitor and enforce its orders. FISA codifies the FISC's enforcement jurisdiction: "Nothing in this chapter shall be construed to reduce or contravene the inherent authority of the [FISC] to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court." 50 U.S.C. § 1803(h).

[110] *See* DEP'T OF JUSTICE, *Sections & Offices*, "Oversight Section," https://www.justice.gov/nsd/sections-offices#oversight:

> The Department of Justice bears the responsibility of overseeing the foreign intelligence, counterintelligence and other national security activities of the United States Intelligence

of Justice states that under Oversight Section monitoring, "instances of non-compliance with [FISC] orders are tracked, timely reported to the FISC and resolved."[111]

b. *Regular Joint DOJ/ODNI Audits*

[57] At regular intervals, the Department of Justice's National Security Division (DOJ NSD) and the Office of the Director of National Intelligence (ODNI) jointly audit US intelligence agencies' compliance with FISC orders relating to programs under Section 702. The joint audit is conducted on-site:

> Currently, at least once every two months, [DOJ] NSD and ODNI conduct oversight of NSA, FBI, and CIA activities under Section 702 [FISA]. These reviews are normally conducted on-site by a joint team from [DOJ] NSD and ODNI. The team evaluates and (where appropriate) investigates each potential incident of noncompliance, and conducts a detailed review of agencies' targeting and minimization decisions. The Department of Justice reports any incident of noncompliance with the statute, targeting procedures, and minimization procedures to the FISC, as well as to Congress.[112]

[58] Moreover, the "the NSD and ODNI team lead weekly calls and bimonthly meetings with representatives from the NSA, CIA, and FBI to discuss, among other things, compliance trends and incidents that affect multiple agencies."[113]

c. *Periodic DOJ/ODNI Joint Reports*

[59] Using the results of their audits, the DOJ and the ODNI jointly issue quarterly compliance reports directly to the FISC.[114] In addition to quarterly reports, the DOJ and the ODNI issue semi-annual reports on NSA compliance with targeting procedures, minimization procedures, and acquisition guidelines set forth in FISC orders governing Section 702 programs.[115] These reports set forth the "scope, nature, and actions taken in response to

---

> Community to ensure compliance with the Constitution, statutes and Executive Branch policies. [. . .] The Oversight Section of the National Security Division's Office of Intelligence is charged with meeting this responsibility by monitoring the activities of various Intelligence Community elements. To accomplish this, the Oversight Section identifies individual and systemic incidents of non-compliance, and then works with the responsible agencies to correct existing problems, as well as to limit the occurrence of future incidents. [] In addition to its broad intelligence collection oversight responsibilities, the Oversight Section also fulfills various reporting obligations of the Department. For example, the Oversight Section ensures that instances of non-compliance with Foreign Intelligence Surveillance Court (FISC) orders are tracked, timely reported to the FISC and resolved.

[111] *See id*.
[112] *See Joint Statement*, *supra* note 65.
[113] *See* PCLOB 702 REPORT, *supra* note 66, at 74.
[114] *Id.* at 29 n.97.
[115] *Joint Statement*, *supra* note 65, at 7. Notably, at least four of the DOJ/ODNI joint semiannual assessments have been declassified and are available to the public. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF

compliance incidents."[116] DOJ/ODNI reports are available to the FISC when it reviews surveillance applications, or rules on remedial measures after receiving noncompliance notifications. Recently declassified FISC opinions show the FISC has reviewed these reports in deciding whether to approve government requests to authorize surveillance.[117]

d. *Oversight and Reporting within Surveillance Agencies (NSA, CIA, FBI)*

[60] US agencies that conduct surveillance maintain internal compliance policies, oversight procedures, and incident-reporting training. For example, the NSA has policies that require its analysts to report compliance incidents to the Department of Justice and the Director of National Intelligence.[118] NSA analysts must undergo yearly training on legal and internal-policy requirements to report compliance incidents.[119] Analysts who fail to meet ongoing training standards can lose the ability to access data.[120]

[61] Furthermore, four internal NSA units are tasked with monitoring compliance with FISC orders and applicable laws:

JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR JUNE 1, 2012 TO NOVEMBER 30, 2012 (2013), https://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR JUNE 1, 2009 TO NOVEMBER 30, 2009 (2010), http://www.dni.gov/files/documents/FAA/SAR%20May%202010%20Final%20Release%20with%20Exemptions.pdf; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR DECEMBER 1, 2008 TO MAY 31, 2009 (2010), http://www.dni.gov/files/documents/FAA/SAR%20December%202009%20Final%20Release%20with%20Exemptions.pdf; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR SEPTEMBER 4, 2008 TO NOVEMBER 30, 2008 (2009), http://www.dni.gov/files/documents/FAA/SAR%20March%202009%20Final%20Release%20with%20Exemptions.pdf; *see also* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Release of Joint Assessments of Section 702 Compliance*, IC ON THE RECORD (July 21, 2016), https://icontherecord.tumblr.com/post/147761829243/release-of-joint-assessments-of-section-702.

[116] PCLOB 702 REPORT, *supra* note 66, at 29.

[117] *See [Caption Redacted]*, No. [Redacted] (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (noting that the FISC had "examined quarterly compliance reports" in deciding whether to reauthorize Section 702 programs); *[Caption Redacted]*, No. [Redacted] at 3 (F.I.S.C. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf (also noting that the FISC had "examined quarterly compliance reports" in deciding whether to reauthorize Section 702 programs).

[118] The NSA does not directly report compliance incidents to the FISC. The NSA reports compliance incidents to the Department of Justice and the Director of National Intelligence, and the Department of Justice – consistent with its role in representing the executive branch before courts – reports incidents to the FISC. The FISC, however, may require the NSA to appear via an appropriate representative, or to provide written declarations or other evidence, in response to a compliance incident. *See supra* section I.

[119] *See* NSA DIR. OF CIVIL LIBERTIES AND PRIVACY OFFICE, NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, 3 (Apr. 16, 2014), https://www.nsa.gov/about/civil-liberties/reports/assets/files/nsa_report_on_section_702_program.pdf.

[120] *Id.* at 5.

(1) the NSA Office of the Director of Compliance;
(2) the NSA's Office of General Counsel;
(3) the Signals Intelligence Directorate's Oversight and Compliance section; and
(4) the NSA Director of Civil Liberties and Privacy Office.[121]

The NSA Office of Director of Compliance conducts risk assessments to identify potential systemic incidents of noncompliance, and coordinates programs to check that factual representations made to the FISC remain accurate.[122] The NSA Office of General Counsel, and the SIGINT Directorate's Oversight and Compliance section, investigate and report potential incidents of noncompliance.[123] My understanding is that the NSA has over 300 employees dedicated to compliance.

2. Compliance Incident Reporting Requirements

[62] In addition to the monitoring and reporting outlined above, FISC rules and FISC orders require the government to report compliance incidents to the FISC. The FISC Rules of Procedure require government agencies to "immediately" report compliance incidents to the FISC.[124] This notification must identify:

(1) the compliance incident at issue;
(2) all facts and circumstances relevant to the non-compliance;
(3) the government's proposed solution to the compliance incident; and
(4) what the government proposes to do with information obtained via noncompliance.[125]

The government must also "immediately" submit a similar notification if it learns that any aspect of a prior FISC submission now constitutes a "misstatement or omission of material fact."[126]

---

[121] PCLOB 702 REPORT, *supra* note 66, at 66-67.
[122] *See id.* at 67.
[123] *Id.*
[124] F.I.S.C. R.P. 13(b): "If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law, the government, in writing, must immediately inform the Judge to whom the submission was made."
[125] *Id.* 13(b)(1)-(4). It is worth noting that for Section 702 programs, standard NSA, CIA, and FBI procedures require these agencies to immediately purge any information they identify as having been collected as a result of noncompliance. Within the NSA, this deletion requirement can only be waived by the Director of the NSA on a communication-by-communication basis. *See* PCLOB 702 REPORT, *supra* note 66, at 49. ("If the data was acquired as a result of a compliance incident . . . the acquired communications must be purged.")
[126] F.I.S.C. R.P. 13(a): "If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the government, in writing, must immediately inform the Judge to whom the submission was made of: (1) the misstatement or omission; (2) any necessary correction; (3) the facts and circumstances relevant to the misstatement or omission; (4) any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and (5) how the government proposes to dispose of or treat any information obtained as a result of the misstatement or omission."

[63] In addition to FISC Rules of Procedure, Section 702 programs are subject to targeting and minimization procedures approved by the FISC. FISC decisions require government agencies to report any instance of noncompliance with these procedures.[127]

[64] When compliance incidents are identified, the DOJ – in order to satisfy its obligation to report "immediately" – will sometimes contact FISC staff attorneys via telephone and provide an oral notification.[128] Thereafter, the government will supplement its initial notification with a written submission setting forth the required information as well as any remedial actions the government has implemented.

3. The Result: Timely and Reliable Compliance Reporting

[65] The above system of rules, audits, and reports are designed to ensure that compliance incidents are reported to the FISC for review. Recent FISC opinions appear to reflect general satisfaction with the timeliness and reliability of compliance reporting. As the FISC stated in 2014, "[i]t is apparent to the Court that the implementing agencies, as well as the Director of National Intelligence [] and [the Department of Justice's National Security Division], devote substantial resources to their compliance and oversight responsibilities," and that as a result, "instances of noncompliance are identified promptly and appropriate remedial actions are taken."[129]

B. FISC Responses to Noncompliance

[66] When the FISC receives reports of compliance incidents, it has imposed significant sanctions. FISC compliance practice has resulted in substantial changes to surveillance programs, as well as the termination of one NSA collection program. This part will summarize FISC opinions that illustrate how the FISC has responded to government noncompliance.

1. The 2009 Judge Walton Opinions

[67] In a series of 2009 opinions, FISC Judge Reggie Walton issued a series of opinions addressing a compliance issue related to the NSA's then-existing telephony metadata program. These opinions required the government to appear and explain its noncompliance, restricted the NSA from accessing the telephony metadata, and helped lead to the NSA adopting compliance-management practices.

---

[127] The 2009 FISC opinion setting forth this reporting requirement is still classified, but has been disclosed to the Privacy and Civil Liberties Oversight Board. *See* PCLOB 702 REPORT, *supra* note 66, at 29-30.
[128] *See* Chief Judge Walton Letter, *supra* note 16, at 2-3.
[129] *[Caption Redacted]*, No. [Redacted] at 28 (F.I.S.C. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

a. *Background*

[68] In 2009, the NSA discovered that technical systems related to a telephony metadata collection program, which existed at that time, were automatically updating an "alert list" of phone numbers. The updated alert list was automatically run against incoming metadata, and the automatically-updated portion of the list was a violation of FISC requirements that NSA analysts individually determine which phone numbers were reasonably associated with terrorist suspects. The Department of Justice reported the NSA's "alert list" compliance incident to the FISC on January 15, 2009, announcing that as a result of this discovery, the NSA would be conducting an end-to-end review of technical systems related to the telephony metadata program.

b. *The FISC's First Compliance Order and the Government's Response*

[69] The FISC's response evinced concern for noncompliance. It noted that the "alert list" query procedure "appears to the Court to be directly contrary to" governing FISC orders. The FISC stated it was "exceptionally concerned about what appears to be a flagrant violation of its Order[s] in this matter."[130]

[70] As a result, the FISC indicated it was considering terminating the metadata collection program, as well as holding executive officials in contempt. The FISC ordered the government to submit briefing so that it could determine:

(1) whether the FISC orders underlying the metadata program "should be modified or rescinded;"
(2) whether any "other remedial steps should be directed;" and
(3) whether the FISC should take action against "persons responsible for any misrepresentations to the Court," including through the FISC's contempt powers or by referring individuals to professional oversight offices.[131]

[71] To make these determinations, the FISC ordered the government to respond to questions, and to support its answers with sworn declarations of executive branch officials. The FISC's questions included:

- How long has the "alert list" procedure been conducted?
- Who within the executive branch – identified by name and title – knew about the "alert list" procedure, and for how long had they known?
- What oversight mechanisms were used to identify the "alert list" procedure, and why was it not discovered earlier?
- How does the "alert list" generate the phone numbers it queries?

---

[130] *In re Production of Tangible Things from [Redacted]*, No. BR 08-13, 2009 WL 9157881 at 2 (F.I.S.C. Jan. 28, 2009), https://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf.

[131] *Id.* at 2.

- Is the government technically able to purge all information derived from "alert list" queries?[132]

[72] The government submitted responsive briefing to the FISC on February 17, 2009, supported by a declaration of the Director of the NSA. The NSA explained that the systems underlying the telephony metadata program were complex, such that no senior official within the agency had had a "complete technical understanding" of how NSA systems interacted with telephony metadata the NSA received.[133] As a result, the NSA stated that no official had realized the "alert list" procedure was being used in a manner inconsistent with governing FISC orders.

---

[132] *Id.* at 3-4. Verbatim, the FISC's questions were as follows:

> 1. Prior to January 15, 2009, who, within the Executive Branch, knew that the "alert list" that was being used to query the Business Record database included telephone identifiers that had not been individually reviewed and determined to meet the reasonable and articulable suspicion standard? Identify each such individual by name, title, and specify when each individual learned this fact.
>
> 2. How long has the unauthorized querying been conducted?
>
> 3. How did the unauthorized querying come to light? Fully describe the circumstances surrounding the revelations.
>
> 4. The application signed by the Director of the Federal Bureau of Investigation, the Deputy Assistant [Attorney General] for National Security, the [Department of Justice], and the Deputy [Attorney General] of the United States as well as the Declaration of [redacted], a Deputy Program Manager at the NSA, represents that during the pendency of this order, the NSA Inspector General, the NSA General Counsel, and the NSA Signals Intelligence Directorate Oversight and Compliance Office each will conduct reviews of this program. The Court's Order directed such review. Why did none of these entities that were ordered to conduct oversight over this program identify the problem earlier? Fully describe the manner in which each entity has exercised its oversight responsibilities pursuant to the Primary Order in this docket as well as pursuant to similar predecessor Orders authorizing the bulk production of telephone metadata.
>
> 5. The preliminary notice from [the Department of Justice] states that the alert list includes telephone identifiers that have been tasked for collection in accordance with NSA's SIGINT authority. What standard is applied for tasking telephone identifiers under NSA's SIGINT authority? Does NSA, pursuant to its SIGINT authority, task telephone identifiers associated with United States persons? If so, does NSA limit such identifiers to those that were not selected solely upon the basis of First Amendment protected activities?
>
> 6. In what form does the government retain and disseminate information derived from queries run against the business records data archive?
>
> 7. If ordered to do so, how would the government identify and purge information derived from queries run against the business records data archive using telephone identifiers that were not assessed in advance to meet the reasonable and articulable suspicion standard?

Id. (internal citations omitted).

[133] *In re Production of Tangible Things from [Redacted]*, No. BR 08-13 at 8, https://www.eff.org/files/filenode/br_08-13_order_3-2-09_final_redacted.ex_-_ocr_1.pdf.

[73] The NSA further stated it had implemented a "technical safeguard" that would prevent "any automated process or subroutine" (such as the alert list) from accessing metadata.[134] The NSA requested that the FISC not order any remedial measures.

c. *The FISC's Second Compliance Order*

[74] The FISC responded to the NSA's noncompliance by imposing substantial restrictions on the metadata program. The FISC prohibited the NSA from accessing the telephony metadata database. In order to query the database, the FISC required the NSA to first file a motion and receive FISC approval for every selector the NSA wished to query.[135]

[75] The FISC justified its response by stating that to approve a program like the metadata program, it "must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders."[136] The FISC reviewed compliance incidents that had been reported relating to the metadata program from 2006 onwards.[137] The FISC noted that since the NSA's end-to-end review of technical systems was still ongoing, "no one inside or outside of the NSA [could] represent with adequate certainty" whether the NSA's proposed technical fixes would ensure compliance.[138] Thus, the FISC stated it "no longer ha[d] confidence" that NSA leaders could ensure compliance, and that "[m]ore is required" than technical measures.[139]

[76] The FISC stated its prohibition on the NSA accessing the metadata database would remain in force "until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data."[140]

d. *The FISC's Third Order*

[77] Approximately seven months later, the NSA had resolved compliance issues to the FISC's satisfaction. By that time, the NSA had completed its end-to-end review of telephony metadata systems. It identified compliance issues, and provided the FISC with a report of how it intended to ensure compliance going forward.[141] Among other measures, the NSA adopted compliance-management procedures. These included creating records of decisions to query a

---

[134] *Id.* at 14.
[135] *Id.* at 18-19. The FISC permitted the NSA to access the database without prior approval in cases of emergency posing a danger to human life, but required the NSA to immediately report any such queries to the FISC.
[136] *Id.* at 12.
[137] *Id.* at 10.
[138] *Id.* at 15.
[139] *Id.* at 17.
[140] *Id.* at 18.
[141] The Obama Administration has declassified the NSA's report of its end-to-end systems review that it provided to the FISC. *See In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 09-09 (F.I.S.C. filed Aug. 17, 2009), https://www.dni.gov/files/documents/section/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf.

selector; conducting decision reviews; logging analyst activity to create audit trails; and audits.[142] The NSA also introduced compliance training as a condition for analysts' ability to search metadata, or to view the results of search queries.[143]

[78] On September 3, 2009, Judge Walton entered an order that reauthorized the telephony metadata program.[144] This order lifted the prohibition on the NSA's ability to query the metadata database, provided that NSA analysts first determined that there was a "reasonable and articulable suspicion" that telephone numbers to be searched were associated with terrorism suspects.[145]

e. *The FISC's Final Compliance Order*

[79] Following the FISC's September 3, 2009 order, the Department of Justice reported two additional compliance incidents to the FISC. Results of metadata queries had been shared with an NSA analyst who had not yet received now-mandatory training on compliance with FISC orders.[146]

[80] The FISC responded it was "deeply troubled" by these incidents, which occurred "only a few weeks" after the NSA had submitted a "report intended to assure the Court that NSA had addressed and corrected [compliance] issues . . . and had taken the necessary steps to ensure compliance with the Court's orders going forward."[147] On Friday, September 25, 2009, the FISC ordered the NSA to appear in person the following Monday to explain the compliance incidents under oath. The FISC's order again indicated it was considering terminating or restricting the metadata program.

[81] Judge Walton's order compelling the NSA to appear shows the authority that the FISC has exercised when it believes serious compliance issues need to be addressed. Verbatim, it reads:

> [THE COURT] HEREBY ORDERS that representatives of the NSA and [the Department of Justice's National Security Division (NSD)] appear for a hearing on Monday, September 28, 2009, at 3:30 p.m., the purpose of which will be to inform the Court more fully of the scope and circumstances of the incidents discussed above, and to allow the Court [to] assess whether the Orders issued in this docket should be modified or rescinded and whether other remedial steps

---

[142] *See In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 09-13, 2009 WL 9150914 at 3 (F.I.S.C. Sept. 3, 2009), at 3, https://www.dni.gov/files/documents/section/pub_Sep%203%202009%20Primary%20Order%20from%20FISC.pdf.
[143] *Id*. at 4-5.
[144] *See id.*
[145] *Id*. at 1-3.
[146] *In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 09-13, 2009 WL 9150896 at 1 (F.I.S.C. Sept. 25, 2009), https://www.dni.gov/files/documents/section/pub_Sept%2025%202009%20Order%20Regarding%20Further%20Compliance%20Incidents.pdf.
[147] *Id*. at 2.

> should be imposed. The Court expects that the representatives of the NSA and NSD who appear at the hearing will include persons with detailed knowledge of the facts and circumstances surrounding the above-described incidents and why remedial measures had not been implemented to ensure compliance with the Court's Orders that have been issued in this docket, as well as officials of stature sufficient to speak authoritatively on behalf of the Executive Branch.[148]

[82] Following the hearing, the FISC was able to resolve its concerns. The telephony metadata program was discontinued in 2015, after passage of the USA FREEDOM Act prohibited bulk collection under Section 215.

2. The 2009/2010 Internet Metadata Program Opinions

[83] In a second series of FISC orders, the FISC addressed compliance issues related to an Internet metadata collection program that existed until 2010. In response to noncompliance reports, the FISC imposed weekly reporting requirements on the NSA. Then, following the Department of Justice's notification of a significant compliance incident, questioning by the FISC resulted in the NSA electing to terminate the Internet metadata program.

a. *Background*

[84] During the 2009-2010 period, the NSA operated an Internet metadata collection program. Under FISC orders, the NSA was not generally permitted to share Internet metadata with other agencies. The NSA was also not permitted to disseminate Internet metadata that contained information about US persons to other agencies, unless the NSA's Chief of Information Sharing determined that the information was (1) related to counterterrorism information, and (2) necessary to understand the counterterrorism information or assess its importance.

[85] On June 16, 2009, the Department of Justice reported to the FISC that the NSA had failed to make the appropriate determinations before disseminating US person information to other agencies.[149] The Department of Justice also informed the FISC that in some cases, results of metadata queries had been uploaded into a database that other agencies could access.[150]

b. *The FISC's First Compliance Opinion*

[86] The FISC's response showed concern for noncompliance. The FISC stated it was "gravely concerned" that "NSA analysts, cleared or otherwise, have generally *not* adhered to the dissemination restrictions" contained in FISC orders.[151] The Court stated that it "seems clear" that the NSA had "failed to satisfy its obligation to ensure that all analysts with access to

---

[148] *Id.* at 2.
[149] *[Caption Redacted]*, No. PR/TT [Redacted] at 4-5 (F.I.S.C. June 22, 2009), https://www.dni.gov/files/documents/1118/CLEANED101.%20Order%20and%20Supplemental%20Order%20%286-22-09%29-sealed.pdf.
[150] *Id.* at 5.
[151] *Id.* at 6 (emphasis in original).

information derived from [Internet] metadata 'receive appropriate training and guidance regarding . . . *the retrieval, storage, and dissemination of such information*.'"[152] The FISC also expressed "seriou[s] concer[n]" that the NSA had placed Internet metadata into "databases accessible by outside agencies," which the FISC noted "violates not only the Court's orders, but also the NSA's minimization and dissemination procedures."[153]

[87] As a remedy, the FISC imposed weekly reporting requirements on the NSA. Every Friday going forward, the NSA was ordered to file a report "listing each instance during the seven-day period ending the previous Friday in which NSA has shared, in any form, information obtained or derived from the [Internet] metadata collections with anyone outside NSA" – specifying the date of dissemination, the recipient, and the form in which the data was communicated.[154] Additionally, for any instance where US person information was disseminated, the FISC required the NSA's Chief of Information Sharing to submit a certification that, "prior to dissemination," he had determined that the information was related to counterterrorism information, and was necessary to understand the counterterrorism information or assess its importance.

c. *The NSA's Second Compliance Incident Report*

[88] At approximately the same time that the above compliance incidents were reported, the NSA conducted an end-to-end review of technical systems related to the Internet metadata program. The review discovered collection irregularities, which the NSA reported to the Department of Justice's National Security Division. The Department of Justice notified the FISC that a compliance issue was forthcoming and investigated further. [155]

[89] Subsequent filings indicate the Department discovered there was a substantial overcollection issue affecting most of the NSA's metadata records. The Department of Justice reported to the FISC that "many other types of data" had been collected, and that "virtually every" metadata record included some data that had not been authorized for collection by the FISC.[156] The Department did not provide an explanation for the overcollection; the FISC stated that "the most charitable interpretation" was that "poor management" and "non-communication with the technical personnel" were the cause.[157]

[90] Following this compliance incident notification, the NSA submitted an application asking the FISC to reauthorize the Internet metadata program. The NSA proposed that it would not

---

[152] *Id.*
[153] *Id.* at 6-7.
[154] *Id.* at 7.
[155] The Obama Administration has declassified the DOJ's preliminary notice of a compliance incident, *see Preliminary Notice of a Potential Compliance Incident Involving [Redacted]*, (F.I.S.C. filed [date redacted]), https://www.dni.gov/files/0808/Final%20037.Preliminary%20Notice%20of%20Potential%20Compliance%20Incident.pdf. In this notice, the NSA advised that it would not query the Internet metadata database "until the matter is resolved and with the [FISC's] express approval." *Id.* at 3.
[156] *See [Caption Redacted]*, No. PR/TT [Redacted] at 20-21 (F.I.S.C. [Date Redacted]), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[157] *Id.* at 21.

permit its analysts to query Internet metadata it had previously collected, and that previously collected Internet metadata would be segregated.[158]

d. *The FISC's Response*

[91] FISC Judge Reggie Walton, reviewed the NSA's application requesting reauthorization. Judge Walton advised the NSA he was concerned about the legality of the NSA's Internet metadata program, and scheduled a hearing. As a result of Judge Walton's questioning, the NSA elected "not to submit a final application" – thus permitting the Internet metadata program to terminate.[159] Following the program's expiration, the FISC ordered that the NSA could not "access the [Internet metadata previously] obtained for any analytic or investigative purpose."[160] The NSA terminated the program in the wake of the FISC's stated concerns about the program's legality.

3. The 2011 Upstream Program Opinions

[92] A third series of FISC opinions address a compliance issue that arose in the NSA's Upstream program. In response to NSA noncompliance, the FISC threatened program closure. The FISC's response led the NSA to make substantial changes to a long-running intelligence program, and these remain in force today.

a. *Background*

[93] In April 2011, the government filed a certification to reauthorize Section 702 programs. As I explain in more detail in Chapter 3, one part of Section 702 collection is known as the "Upstream" program, in which NSA acquires communications that are to, from, or about an approved selector as they travel through the Internet backbone.[161]

[94] In its April 2011 certification for reauthorization, the government informed the FISC that Upstream systems did not acquire discrete communications, but instead so-called "Internet transactions."[162] Internet transactions are a complement of data packets that can contain single or multiple communications.[163] If the latter, they are referred to as Multiple Communication

---

[158] *Id.* at 22.
[159] *See id.* at 22-23.
[160] *See [Name Redacted]*, No. PR/TT [Redacted] and Previous Dockets (F.I.S.C. [date redacted]), at 4. https://www.dni.gov/files/0808/Final%20006.FISC%20Supplemental%20Order.pdf. Judge Walton permitted the NSA to access the stored Internet metadata if doing so was "necessary in order to protect against an imminent threat to human life," but if it did so, the NSA was required to provide a written report to the FISC. *Id.* Later, FISC Judge Bates permitted the NSA to query portions of the Internet metadata to the extent that (a) at the time of collection, the government did not know, or have reason to know, that other types of data were being collected; and if (b) the NSA segregated searchable from non-searchable metadata and provided the FISC with monthly reports on its efforts to do so. *[Caption Redacted]*, No. PR/TT [Redacted] at 114-117 (F.I.S.C. [Date Redacted]), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[161] *See* Chapter 3, Section III(C)(3).
[162] *[Caption Redacted]*, No. [Redacted], 2011 WL 10945618 at 5 (F.I.S.C. Oct. 3, 2011) (Mem. Op.), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.
[163] *See id.* at 28-29 n. 23.

Transactions (MCTs). While MCTs contain emails or other communications sent to or from a targeted individual, they can also contain further communications that are unrelated to the person targeted for surveillance.

b. *The NSA's Compliance Incident Report and Reauthorization Request*

[95] The NSA's notification that it was collecting transactions, as opposed to communications, resulted in a months-long investigation by the FISC, discussed in more detail in part I.B.2. above.[164] The investigation revealed that present technology was unable to discern which Internet transactions constituted MCTs – and also whether particular MCTs contained communications from non-targeted persons. As a result, Upstream collected some emails of non-targeted individuals.

[96] The FISC eventually required the NSA to submit statistical analyses of Upstream collection for its review. The FISC determined that a small, but non-trivial percentage of Upstream collections constituted MCTs containing communications of non-targeted persons.[165] The NSA acknowledged this was the case, but stated that a technical solution was not available because acquisition systems could only capture transactions, not individual communications. The NSA therefore asked the FISC to reauthorize Upstream without any changes.

c. *The FISC's Response*

[97] The FISC refused to reauthorize Upstream in its then-current form, instead requiring the NSA to either change or terminate the program. Its opinion evinced concern for the NSA's compliance with its orders.

[98] The FISC began its analysis by, first, indicating it was concerned that Upstream collection appeared to be more expansive than the government had represented in the past. The FISC reviewed the NSA's record of non-compliance with FISC orders, including the 2009 Judge Walton opinions relating to the telephony metadata program summarized in part II.B.1. above. The FISC stated it was "troubled" that the Upstream issues marked what it saw as another "substantial misrepresentation" about "the scope of a major collection program."[166]

---

[164] To summarize the FISC's investigation, the FISC (1) posed two sets of follow-up questions to the government; (2) met with senior Department of Justice officials; (3) required the government to submit a statistically representative sample of Upstream collection; (4) received approximately five separate written submissions from the government; and (5) held a hearing to discuss the government's statistical analysis and its implications. *See supra* section I(B)(2).

[165] *[Caption Redacted]*, No. [Redacted], 2011 WL 10945618 at 33-34 (F.I.S.C. Oct. 3, 2011) (Mem. Op.), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. The FISC described the percentage as "relatively small;" of approximately 13.25 million Internet transactions Upstream acquired in a six-month period, the FISC stated that 996 to 4,965 were MCTs that contained wholly domestic communication not to, from, or about a tasked selector. *See id*. at 33 n.31, 34 n.32.

[166] *Id*. at 16 n.14.

[99] Second, the FISC reviewed Upstream's minimization procedures and determined they did not minimize the number of emails belonging to non-targeted persons that the NSA retained. The FISC stated that the "NSA could do substantially more to minimize the retention" of non-target communications.[167] As an example, the FISC stated it was "unclear" why NSA analysts would not be required to delete non-target communications that did not contain foreign-intelligence information. The FISC also noted that the NSA had not demonstrated "why it would not be feasible to limit access to [U]pstream acquisitions to a smaller group of specially-trained analysts who could develop expertise in identifying and scrutinizing MCTs" to remove non-target communications.[168]

[100] Lastly, the FISC applied the Fourth Amendment's reasonableness framework and determined that Upstream's collection of MCTs was not consistent with the US Constitution. The Court noted that although a relatively small number of non-target emails were affected via MCT acquisition, "the intrusion resulting from [the] NSA's acquisition of MCTs is substantial."[169] In the FISC's eyes, it was difficult to justify this intrusion because "the communications of concern here" were not acquired to protect national security, but "simply because they appear somewhere" in a transaction where a targeted facility also appeared.[170] Thus, the FISC held they "do not serve the national security needs" underlying the Upstream program.[171] Given that the FISC had determined the NSA's minimization procedures "tend to maximize the retention of" non-target communications, they "enhanc[ed] the risk" that intrusions on privacy interest would continue to occur.[172] As a result, the FISC stated it was "unable" to conclude that Upstream, in its present form, was reasonable under the Fourth Amendment.[173]

[101] The FISC therefore declined to reauthorize the Upstream program in regards to MCT collection. Instead, the FISC gave the NSA 30 days in which it could (a) "correct the deficiencies" the FISC had identified, or (b) terminate the MCT collection portion of Upstream.[174] With this order, the FISC effectively threatened program termination if the NSA could not remedy the problems the FISC had identified.

d. *The NSA Changes the Upstream Program in Response to the FISC's Order*

[102] The FISC's order led the NSA to propose substantial changes to the Upstream program. Going forward, the NSA agreed to:

(1) reduce the retention period for Upstream-collected transactions by three years;

---

[167] *Id.* at 61.
[168] *Id.*
[169] *Id.* at 72.
[170] *Id.* at 76.
[171] *Id.* at 78.
[172] *Id.*
[173] *Id.*
[174] *See [Caption Redacted]*, No. [Redacted], 2011 WL 10945618 at 3-4 (F.I.S.C. Oct. 3, 2011) (Order), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

(2) segregate Upstream-collected MCTs containing potentially protected communications into a separate database;
(3) only permit NSA analysts who had received MCT review training to access the MCT database;
(4) immediately destroy any MCTs containing wholly domestic communications; and
(5) flag all other MCTs as having emanated from the MCT database, thus requiring NSA analysts to make – and document – a series of determinations before using them.[175]

Moreover, the NSA agreed that Upstream-collected data would not be shared with any other agency.[176]

[103] The FISC concluded that these measures adequately protected the non-target communications embedded within MCTs "that are most likely to contain non-target information subject to statutory or constitutional protection."[177] These measures have remained in place for the Upstream program since their adoption in 2011 until the present.[178]

e. *The NSA Purges Previously-Acquired Upstream Data*

[104] At the same time it approved the NSA's changes to Upstream, the FISC ordered the NSA to explain what it intended to do with MCTs the Upstream program had previously collected. The FISC indicated that it intended to evaluate whether use of earlier-collected MCTs would violate 50 U.S.C. § 1809(a)(2), which makes it a crime to "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through" unauthorized means of surveillance.[179] In response to the FISC's questions, the NSA voluntarily deleted all data Upstream had collected prior to October 31, 2011.[180]

4. Conclusion: the FISC Imposes Significant Penalties on Noncompliance

[105] The record shows evolution over time in the comprehensiveness of FISC oversight of the agencies and their surveillance programs. After the attacks of September 11, 2001, the US

---

[175] *See [Caption Redacted]*, No. [Redacted], 2011 WL 10947772 at 4-5 (F.I.S.C. Nov. 30, 2011), http://www.fas.org/irp/agency/doj/fisa/fisc1111.pdf.
[176] PCLOB 702 REPORT, *supra* note 66, at 54.
[177] *[Caption Redacted]*, No. [Redacted], 2011 WL 10947772 at 6 (F.I.S.C. Nov. 30, 2011), http://www.fas.org/irp/agency/doj/fisa/fisc1111.pdf.
[178] PCLOB 702 REPORT, *supra* note 66, at 41 *et seq*. The 2015 NSA minimization procedures reflecting these safeguards have been declassified, *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, MINIMIZATION PROCEDURES USED BY THE NSA IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (July 15, 2015), https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf.
[179] *See [Caption Redacted]*, No. [Redacted] at 29-30 (F.I.S.C. Sept. 25, 2012), https://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.
[180] *Id*. at 30.

government initiated new surveillance programs, including programs using new powers under the USA PATRIOT Act and the warrantless wiretapping program called StellarWind. For StellarWind, as discussed in section I.C. of this Chapter, the FISC initially had no notice of its existence. Once it did, the FISC found that the program did not have a lawful basis, and refused to approve the program until new statutes were enacted in 2007 and 2008. In the period after 2001, the FISC also approved government actions that, in retrospect, were broader than I think was a fair reading of a statute, such as the 2004 approval of the Internet metadata program.[181]

[106] Over time, however, the FISC established stricter oversight and insisted on a far more comprehensive compliance program. The FISC's compliance opinions show a clear record since 2009 of imposing significant sanctions for noncompliance with its orders. The FISC's responses to compliance incidents have resulted in (1) the termination of the NSA's Internet metadata collection program; (2) substantial modifications to the Upstream program; (3) the deletion of data collected via Upstream prior to October 2011; and (4) a temporary prohibition on the NSA accessing its telephony metadata database.

[107] I believe that a fair reading of the record, based on the material declassified since 2013, shows that the FISC now oversees a comprehensive compliance system. Recent FISC opinions have expressed satisfaction with surveillance agencies' compliance efforts, stating that "instances of noncompliance are identified promptly and appropriate remedial actions are taken."[182] In my view, the independent federal judges on the FISC have learned from the experiences since 2001, and today oversee a compliance program that I believe is unmatched for any other national intelligence service.

III. Increased Transparency about US Surveillance through the FISC's Initiative and Recent Legislation

[108] 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. Moreover, information about the orders issued by the FISC to telecommunications providers was equally secret.

[109] This section describes how, in recent years, the FISC has supported transparency, and how transparency efforts initiated by the FISC have been codified into US surveillance statutes. Part A describes how in response to the Snowden disclosures, the FISC began to release more of its own opinions and procedures, and how USA FREEDOM Act provisions now require important interpretations of law to be published. Part B discusses FISC litigation that led to the first transparency reporting rights since the enactment of FISA, and how the USA FREEDOM Act has codified and expanded those rights.

---

[181] *See [Caption Redacted]*, No. PR/TT [Redacted] (F.I.S.C. [month & day redacted], 2004), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

[182] *[Caption Redacted]*, No. [Redacted] at 28 (F.I.S.C. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

A. The FISC Responded to the Snowden Disclosures by Supporting Transparency, and FISC Transparency is Now Codified in FISA

[110] FISA generally provides that FISC proceedings and rulings are secret. This secrecy was originally mandated on the reasoning that surveillance cannot be effective if targeted individuals know it is coming.[183] In recent years, however, the FISC's role expanded from evaluating case-specific facts to overseeing surveillance programs, and this required the FISC at times to interpret US surveillance laws. Particularly following the Snowden disclosures, there was increased recognition that secret interpretations of law were difficult to reconcile with rule-of-law principles, without providing the national-security benefits FISA secrecy was originally instituted to protect.

[111] This section shows how the FISC, on its own initiative, supported transparency by publishing opinions related to an NSA telephony metadata program, so that policymakers could review them and decide the program's future. It also shows how the FISC supported efforts by third parties to access these opinions. I close by showing how the policy of making significant FISC legal interpretations open to the public, which I supported in print in 2004, is now codified by the USA FREEDOM Act.

1. Background: Publication Orders under FISC Rule of Procedure 62

[112] Although FISC opinions are generally treated as classified, FISC Rule of Procedure 62 permits the FISC judge "who authored an opinion" to request that the opinion be published. When this occurs, the FISC's presiding judge confers with the remaining FISC judges, and can then order that any "order, opinion, or other opinion" be published.[184] (This Chapter refers to such decisions to publish as "publication orders.")

[113] When the FISC orders an opinion to be published, the executive branch is given an opportunity to redact "properly classified information" as it believes is necessary for national security.[185] As will be seen below, the FISC can review governmental redactions. Following the FISC's acceptance of a redacted version of its opinion, the FISC opinion is published.

2. The FISC Responded to the Snowden Disclosures by Publishing Opinions Relevant to Public Debate

[114] Shortly after media outlets began reporting on the Snowden documents, President Obama confirmed the existence of an NSA telephony metadata collection program. Within the US, this began a nationwide public debate about the program's effectiveness and privacy implications.[186]

---

[183] *See* Swire, *supra* note 2, at 1327 (describing FISC secrecy as "a natural outgrowth of [FISA's] purpose, to conduct effective intelligence operations against agents of foreign powers").
[184] F.I.S.C. R.P. 62(a).
[185] *Id.*
[186] The FISC was aware of the telephony metadata program at the time of the Snowden disclosures. The program had been under FISC oversight since 2006.

The FISC responded to this debate by, as it stated in one of its publication orders, "disclos[ing] the Court's legal reasoning" in opinions related to the metadata program to the public.[187] Additionally, the FISC granted standing rights to civil-liberties organizations to seek publication of these opinions, and resisted government attempts to withhold them.

a. *The FISC Published Metadata Opinions on its Own Initiative*

[115] Following President Obama's confirmation of the metadata program's existence, the FISC issued four opinions addressing the program's legal basis prior to reforms introduced by the USA FREEDOM Act in 2015.[188] At the end of each opinion, the FISC determined that – given the debate surrounding the metadata program – its opinion should be made available for review by the public, so that the political branches could determine the program's future. The following provides a brief overview of the opinions and the FISC's reasoning in publishing them:

> *The August 22, 2013 opinion*. On August 22, 2013, the FISC issued its first post-Snowden opinion addressing the legal basis of the telephony metadata program.[189] The FISC judge who authored the opinion recognized that "whether and to what extent the government seeks to continue the [telephony metadata] program . . . is a matter for the political branches of government to decide"—and that "the public interest in this matter" was substantial.[190] The judge therefore requested publication under FISC Rule of Procedure 62. The following day, Presiding FISC Judge Reggie Walton ordered the government to conduct a declassification review.[191] On September 17, 2013 – just under one month after the FISC issued its opinion – the FISC accepted the government's redactions and ordered redacted versions of its opinion to be published.[192]
>
> *The October 11, 2013 opinion*. The FISC's next opinion addressing the telephony metadata program's legal basis issued on October 11, 2013. Again recognizing "the public interest in this matter," the FISC judge who authored the opinion expressly

---

[187] *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, 2014 WL 5442058 at 11 (F.I.S.C. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-7.pdf.

[188] After the passage of the USA FREEDOM Act, the FISC issued an additional opinion addressing the legal basis of the telephony metadata program, *see In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 15-75, Misc. No. 15-01, 2015 WL 5637562 (F.I.S.C. June 29, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR%2015-75%20Misc%2015-01%20Opinion%20and%20Order_0.pdf.

[189] *See In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things [Redacted]*, No. BR 13-109, 2013 WL 5741573 (F.I.S.C. Aug. 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf (The opinion was originally issued on August 22, but after minor corrections was re-issued on August 29, 2013).

[190] *Id.* at 28-29.

[191] *See In re Application of F.B.I for an Order Requiring the Production of Tangible Things [Redacted]*, No. BR 13-109 (F.I.S.C. Aug. 23, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-2.pdf.

[192] *See In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (F.I.S.C. Sept. 17, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-5.pdf.

requested publication under FISC Rule of Procedure 62.[193] Presiding FISC Judge Reggie Walton ordered the government to conduct a declassification review,[194] and three days later, the as-redacted FISC opinion was published.[195]

The March 20, 2014 opinion. In early 2014, the FISC revisited the legal reasoning behind the metadata program in response to a provider challenge to the program's legality. In doing so, FISC issued a third opinion addressing the legal basis of the telephony metadata program on March 20, 2014.[196] In this opinion, the FISC ordered briefing on whether the opinion should be published. Three weeks later, the FISC announced that in light of "the ongoing public debate regarding this program," it would also request publication under FISC Rule of Procedure 62.[197]

The June 19, 2014 opinion. In June 2014, FISC issued what would ultimately be its final opinion analyzing the telephony metadata program's legal basis. The authoring judge again requested publication, citing "the public interest in this particular collection."[198] One week later, the new Presiding FISC Judge Thomas Hogan ordered redacted versions of the opinion to be published.[199]

[116] By the end of this self-initiated disclosure, the FISC had released 130 pages of legal analysis related to the metadata program. The FISC's decision to publish these opinions remained consistent across a number of judges: four separate judges requested that their opinions relating to the metadata program be published, and two different presiding judges approved their requests.[200] I was part of the President's Review Group that, after reviewing the telephony metadata program, recommended the program's discontinuance.[201] The FISC's initiative in

---

[193] *In re Application of the F.B.I for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 13-158 at 6 (F.I.S.C. Oct. 11, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Memorandum-1.pdf.

[194] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things [Redacted]*, No. BR 13-158 (F.I.S.C. Oct. 15, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Order-1.pdf.

[195] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (F.I.S.C. Oct. 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Order-2.pdf.

[196] *See In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 14-01, 2014 WL 5463097 (F.I.S.C. Mar. 20, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR%2014-01%20Opinion%20and%20Order-1.pdf.

[197] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 14-01 at 2 (F.I.S.C. Apr. 11, 2014), https://www.dni.gov/files/documents/BR%2014-01_FISC_April_11_2014_Order.pdf.

[198] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 14-96, 2014 WL 5463290 at 12 (F.I.S.C. June 19, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR%2014-96%20Opinion-1.pdf.

[199] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 14-96 (F.I.S.C. June 26, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR%2014%2096%20Order-1.pdf.

[200] The requesting judges were Judge Claire Eagan (August 2013), Judge Mary McLaughlin (October 2013), Judge Rosemary Collyer (April 2014), and Judge James Zagel (June 2014). The presiding judges who approved publication were Chief Judge Reggie Wilson (August 2013-April 2014) and Chief Judge Thomas Hogan (June 2014). *See supra* notes 179-189.

[201] *See* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE & COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

publishing its opinions aided our work, including enabling our own Report to discuss these issues in unclassified form, and helped lead to what I consider a better approach to metadata acquisition and use in foreign intelligence investigations.

b. *The FISC Granted Standing Rights to Third Parties to Seek Publication of Significant Opinions*

[117] In addition to disclosing significant opinions on its own initiative, the FISC granted standing rights to non-governmental parties to seek publication of FISC opinions relating to the metadata program. This occurred as a result of litigation brought by the American Civil Liberties Union (ACLU), a long-established American civil-liberties organization. One week after President Obama confirmed the existence of a telephony metadata program, the ACLU led a coalition of civil-liberties organizations that filed a motion with the FISC seeking the release of records interpreting Section 215 of the USA PATRIOT Act (which served as the basis for the metadata program).[202]

[118] There were two main issues in the ACLU litigation, each of which the FISC resolved in favor of transparency. The first was whether organizations like the ACLU had standing to file a publication motion with the FISC. US Supreme Court cases generally require anyone requesting relief from US courts to show an injury that is "concrete and particularized."[203] The FISC held that withholding Section 215 opinions from the ACLU – an organization that was clearly active in "legislative and public debates about the proper scope of Section 215[204] – itself "constitute[d] a concrete and particularized injury in fact."[205] The FISC thus held that the ACLU had standing to seek publication of Section 215 opinions.

[119] The second issue was whether organizations like the ACLU should be considered "a party" entitled to move for publication of FISC opinions under FISC Rule of Procedure 62. The FISC held that although the ACLU was not a "party" to the orders at issue, the FISC had inherent authority to control its own records, and that the strong public interest surrounding Section 215 justified hearing the ACLU's publication motion.[206]

[120] After finding that the ACLU had standing, the FISC determined that the substantial public interest in the telephony metadata program favored publishing opinions relating to Section

---

[202] Mot. of the ACLU et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, (F.I.S.C. June 12, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-1.pdf.
[203] *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).
[204] *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 at 8 (F.I.S.C. Sept. 13, 2013), http://www.fas.org/irp/news/2013/09/fisc-091313.pdf.
[205] *Id.* at 9. The FISC also initially determined that one of the ACLU's co-parties, the Yale Law School Media Freedom and Information Access Clinic (MFIAC), had *not* suffered a similar injury in fact because it "submitted no information as to how the release of the opinions would aid its activities, or how the failure to release them would be detrimental." *See id.* After MFIAC presented evidence of its regular participation in national privacy and constitutional debates, however, FISC reversed this finding and permitted MFIAC to participate as a party to the litigation. *See In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (F.I.S.C. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-6_0.pdf.
[206] *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 at 11-12 (F.I.S.C. Sept. 13, 2013), http://www.fas.org/irp/news/2013/09/fisc-091313.pdf.

215, but partially dismissed the ACLU's publication requests to the extent they were already covered by previously-pending Freedom of Information Act (FOIA) proceedings.[207] Notably, in reaching these conclusions, the FISC facilitated third-party participation via *amici curiae* (friends of the court). *Amici* included a group of US Congressional Representatives, as well as leading US media companies such as the New York Times.[208]

[121] The FISC's resolution of the ACLU litigation was significant. The FISC held as a matter of constitutional law that civil-liberties organizations have standing to raise transparency issues before the FISC, and could not be excluded because they were not parties to the underlying proceedings.[209] Publication arguments of this sort would appear to become stronger under new

---

[207] The FISC stated that "the public interest might be served by [] publication" of opinions related to Section 215, and that "[p]ublication would also assure citizens of the integrity of this Court's proceedings." *Id.* at 16-17. Nonetheless, the FISC noted that the ACLU had previously filed a Freedom of Information Act (FOIA) lawsuit in the US District Court for the Southern District of New York in October 2011, which also sought release of Section 215 opinions. The Court cited the common-law "first-to-file" rule and held that, because the New York FOIA suit was filed first, it would dismiss the ACLU's motion "to the extent that it concerns the opinions that are at issue in the FOIA litigation." However, the FISC noted that this solution was "without prejudice" to reinstatement of publication litigation before the FISC "after resolution of the FOIA litigation." The FISC thereby held that the ACLU would have an avenue to make its case for release and/or publication of telephony metadata opinions – either in parallel FOIA litigation or, if unsuccessful there, before the FISC. *See id.* at 15-16.

[208] A coalition of 16 representatives from the US Congress sought leave to participate as *amici curiae* to argue that "[t]he opinions sought [by ACLU] are essential to the proper functioning of the legislative branch of government and an informed public debate." *See* Mot. of US Representatives Amash et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-2.pdf. Additionally, a coalition of leading media companies – including the Associated Press, Dow Jones & Company, The New York Times Company, and Reuters America LLC (collectively, the "Media Companies") – also sought leave to participate as *amici* supporting the ACLU's motion. Mot. of the Reporters Committee for Freedom of the Press et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, -03, -04 (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-4.pdf.
FISC permitted both the Congressional Representatives and the Media Companies to participate as *amici*. *Id.* (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-3.pdf.
The briefs filed by these *amici* have been declassified; *see* (1) Brief of *Amici Curiae* [Media Companies], *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, *In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders & Directives*, No. Misc. 13-04, *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. 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Brief-3.pdf; (2) Brief of *Amici Curiae* [Congressional Representatives], *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (F.I.S.C. 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Brief-1.pdf.

[209] To avoid confusion, I do not mean to imply that in the future, civil-liberties organizations will always be successful when they ask the FISC to publish certain opinions. In its ACLU holding, the FISC stated that it was facing "extraordinary circumstances" as a result of the Snowden disclosures. *See In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 at 12 (F.I.S.C. Sept. 13, 2013), http://www.fas.org/irp/news/2013/09/fisc-091313.pdf. These circumstances permitted the ACLU to "make reasonably concrete, rather than abstract, arguments in favor of publication" and generated a "high level of public and legislative interest" in the FISC's interpretations of Section 215. *Id.* While I do not anticipate that these circumstances will be present in all future publication motions filed with the FISC, they provide a roadmap for civil-liberties organizations that wish to engage in FISC transparency litigation, and civil-liberties organizations' standing to assert publication motions is not in question.

USA FREEDOM Act provisions requiring the FISC to publish novel or significant opinions, which will be discussed in section III.A.3. below.

c. *The FISC Resisted Government Attempts to Withhold Opinions it Ordered Published*

[122] In addition to the decisions outlined above, the FISC's post-Snowden attitude towards transparency can further be seen in how the FISC responded to government attempts *not* to disclose, or to redact, opinions the FISC ordered to be published. Pursuant to the FISC's publication order in the ACLU litigation, the government identified a February 19, 2013 opinion for publication. The FISC ordered the government to conduct a declassification review and prepare it for publication. The government, however, effectively declined to do so, responding that "the Executive Branch has determined that the Opinion should be withheld in full and a public version of the Opinion cannot be provided."[210]

[123] The FISC responded by ordering the government to "submit a detailed explanation of its conclusion that the Opinion is classified in full and cannot be made public, even in a redacted form."[211] Upon receiving this order, the government no longer attempted to withhold the opinion, but instead chose to redact portions that would purportedly endanger an ongoing counterterrorism investigation. When the FISC received the government's first set of proposed redactions, it had "questions about the scope of some redactions" and "why, in some instances, more narrowly tailored redactions would not adequately protect" national security.[212] The FISC ordered government attorneys to meet with FISC staff attorneys to discuss FISC's concerns.[213] At this meeting, FISC attorneys "called to the government's attention each portion of redacted text as to which the Court questioned the basis for, or scope of, the redaction."[214] "[W]ithout exception," the government agreed that every redaction the FISC questioned was "not classified" and "would not jeopardize the ongoing investigation."[215] The government then offered a "Second Redaction Proposal" incorporating the FISC-proposed disclosures, which the FISC accepted because it "achieve[d] the basic objective sought by the [ACLU]: disclosure of the Court's legal reasoning."[216]

[124] The FISC was similarly attentive to government attempts to redact a March 20, 2014 opinion regarding the metadata program's legal basis. After conducting a declassification review of that opinion, the government proposed numerous redactions. The FISC responded by posing

---

[210] *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 at 1-2 (F.I.S.C. Nov. 20, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-5.pdf.
[211] *Id.* at 2.
[212] *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, 2014 WL 5442058 at 6 (F.I.S.C. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-7.pdf.
[213] *Id.*
[214] *Id.* at 11.
[215] *Id.* at 6-7.
[216] *Id.* at 11.

specific questions and ordering the government to "submit a memorandum" in response.[217] The FISC's questions required the government to identify the bases for some redactions, and to address apparent inconsistencies in its redaction decisions.[218]

3. Transparency is Now Codified in US Foreign Intelligence Statutes

[125] The FISC's policy of "disclos[ing] the Court's legal reasoning"[219] in significant opinions to the public has been codified into FISA via amendments contained within the USA FREEDOM Act. Whenever the FISC issues a "decision, order, or opinion" that contains "a significant construction or interpretation of any provision of law," the law now requires the US government to (1) "conduct a declassification review" and to (2) make the FISC decision "publicly available" to the greatest practicable extent.[220] In other words, if a FISC opinion contains a significant or new interpretation of law, it is required by statute to be published.

[126] Under the USA FREEDOM Act's transparency provisions, the government must provide at least some information on FISC opinions containing significant legal interpretations. Even if the government asserts that an opinion must be withheld in full to protect national security, the government must still provide an unclassified public summary of the FISC decision.[221] The summary must set forth "any significant construction or interpretation of any statute, constitutional provision, or other legal authority relied on by the decision."[222]

---

[217] *In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 14-01, 2014 WL 5463107 at 5 (F.I.S.C. Apr. 11, 2014), https://www.dni.gov/files/documents/BR%2014-01_FISC_April_11_2014_Order.pdf.

[218] *See id.* at 5-6. The Court's questions, verbatim, were as follows:

> A. What is the basis for the Government's conclusion that Petitioner's identity as the recipient of the challenged production order [redacted] constitute classified national security information?
> B. With regard to specific redactions:
> (1.) What is the basis for redacting the words, [redacted] in the first line of footnote 3, on page 5 of the March 20, 2014 Opinion and Order?
> (2.) The redaction in line 3 on page 6 of March 20, 2014 Opinion and Order is inconsistent with the proposed redaction of the same sentence in the Government's Response. What is the basis for this inconsistency?
> (3.) What is the basis for redacting [redacted] in lines 3-4 of page 8 of the March 20, 2014 Opinion and Order?
> (4.) What is the basis for redacting the definition "telephony metadata" in footnote 7 on page 11 of the March 20, 2014 Opinion and Order? The Court notes that the definition of "telephony metadata" is unredacted in the declassified versions of the January 23 Primary Order and other Primary Orders in this matter that have been publicly released.

[219] *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, 2014 WL 5442058 at 11 (F.I.S.C. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-7.pdf.

[220] *See* 50 U.S.C. § 1872. In keeping with prior FISC practice, the government may redact national-security information from the opinion prior to publication.

[221] *Id.* § 1872(c)(1).

[222] *Id.* § 1872(c)(2)(A). Additionally, "to the extent consistent with national security," the summary must contain "a description of the context in which the matter arises."

[127] These transparency provisions have resulted in the release of FISC opinions. On August 22, 2016, the US Director of National Intelligence released two opinions – one by the FISC[223] and one by the Foreign Intelligence Surveillance Court of Review[224] – addressing the question of whether Pen Register/Trap-and-Trace surveillance was legally permitted to capture information known as "post-cut-through digits."[225] In its publication notice for these opinions, the Director of National Intelligence stated it was "releasing these two documents pursuant to Section 1872 of [FISA]," *i.e.* the FISA provisions codifying the USA FREEDOM Act's transparency requirements.[226]

[128] Additionally, the USA FREEDOM Act's transparency provisions exist alongside FISC Rule of Procedure 62(a), which continues to permit the FISC to order on its own initiative that opinions be published. The FISC's holding in the ACLU litigation (outlined above) forms the basis for future holdings to permit civil-liberties organizations to file publication motions.

[129] On a closing note, I point out that every FISC opinion cited in this Chapter, save one,[227] can be accessed via an Internet URL. Many FISC opinions are available from the FISC's own website.[228] Additionally, the Director of National Intelligence's "IC on the Record" website publishes FISC opinions upon declassification, alongside a wealth of other recently-declassified materials relating to US surveillance.[229] This is a degree of transparency that few courts, and practically no other surveillance oversight bodies I am aware of, have achieved.

B. Litigation before the FISC Helped Lead to Transparency Reporting Rights that are Now Codified in FISA

[130] In Chapter 3, I discuss how litigation by leading technology companies resulted in important rights to publish corporate transparency reports – reports on the numbers of government requests they receive for user information.[230] As I discuss here, litigation in the FISC played an important role in creating this result, with a notable scale of participation by non-government parties before the FISC.

---

[223] *See In [Redacted] a U.S. Person*, No. PR/TT 2016-[Redacted] (F.I.S.C. Feb. 12, 2016), https://www.dni.gov/files/icotr/PCTD%20FISC-R%20Certification%2020160818%20pdf.pdf.
[224] *See In re Certified Question of Law*, No. FISCR 16-01 (F.I.S.C.R. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf.
[225] For a discussion of PR/TT surveillance and "post-cut-through digits," see *supra* section I.B.5.
[226] *Release of FISC Question of Law & FISCR Opinion*, IC ON THE RECORD (2016), https://icontherecord.tumblr.com/post/149331352323/release-of-fisc-question-of-law-fiscr-opinion.
[227] In note 127, *supra*, I cite a FISC opinion that requires the NSA to immediately report any noncompliance with the targeting and minimization procedures that govern Section 702 programs. This is the only FISC opinion cited within this Chapter that has not yet been declassified. It has, however, been presented to the Privacy & Civil Liberties Oversight Board for their review, and is described in their report on Section 702. *See* PCLOB 702 REPORT, *supra* note 66, at 29-30.
[228] *See* FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Public Filings*, http://www.fisc.uscourts.gov/public-filings.
[229] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Declassified: Release of FISC Question of Law and FISCR Opinion*, IC ON THE RECORD (Aug. 22, 2016), https://icontherecord.tumblr.com/tagged/declassified.
[230] *See* Chapter 3, Section V(E).

[131] This section will briefly sketch the FISC litigation that led to transparency reporting rights, while highlighting the non-governmental participation the FISC permitted. I will close by summarizing the reporting rights companies gained from the litigation, and how these rights have been codified and expanded by the USA FREEDOM Act.

1. Commencement of the Suit

[132] In June 2013, early media reports relating to the Snowden disclosures erroneously alleged that the NSA was "tapping directly into the central servers" of nine leading American technology companies.[231] The affected companies sought ways to mitigate the reputational harm these reports were causing. As part of this effort, Google and Microsoft requested permission from the Department of Justice to publish (1) aggregate totals of FISA orders and FISA directives they had received, and (2) the total number of subscribers that were affected. The Department of Justice responded it would only permit the companies to publish national-security requests as a single number within "requests from all other US local, state and federal law enforcement agencies" – *i.e*. the companies would have had to report NSA requests in the same category as typical police warrants.[232]

[133] Unsatisfied with their inability to provide more granular transparency, Google[233] and Microsoft[234] filed motions for declaratory judgment with FISC.[235] Both companies argued that the Department of Justice's prohibition on publishing aggregate data on national-security process was unconstitutional because it restricted their right to free speech, guaranteed by the First Amendment of the US Constitution.[236]

---

[231] For the original allegations of direct access, *see, e.g.*, Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), 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. For media reports stating that the "direct access" allegations were inaccurate, *see* Declan McCullagh, *No evidence of NSA's 'direct access' to tech companies*, CNET (June 7, 2013), https://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 (June 7, 2013), http://www.businessinsider.com/washington-post-updates-spying-story-2013-6.

[232] Jeffrey Meisner, *Microsoft's U.S. Law Enforcement and National Security Requests for Last Half of 2012*, MICROSOFT TECHNET (June 14, 2013), https://blogs.technet.microsoft.com/microsoft_on_the_issues/2013/06/14/microsofts-u-s-law-enforcement-and-national-security-requests-for-last-half-of-2012/. Also, the Department of Justice only permitted Google and Microsoft to report "for the six-month period of July 1, 2012 thru December 31, 2012." *Id.*

[233] *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. filed June 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-10.pdf.

[234] *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, No. Misc. 13-04 (F.I.S.C. filed June 19, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-04%20Motion-10.pdf.

[235] As outlined in Section III(A) above, the motions for declaratory judgment were filed pursuant to FISC Rule of Procedure 7(d).

[236] *In re Motion for Declaratory Judgment of Google, Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, No. Misc. 13-03 at 3-5 (F.I.S.C. filed June 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-10.pdf; *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, No. Misc. 13-04 at 5-7 (F.I.S.C. filed June 19, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-04%20Motion-10.pdf. The companies argued that

2. A Coalition of Non-Governmental Parties Joins the Litigation

[134] Google and Microsoft's motions attracted the attention of other leading US technology companies. On September 9, 2013, Yahoo[237] and Facebook[238] filed motions for a declaratory judgment, thus joining the Google/Microsoft transparency litigation as additional parties. Like Google and Microsoft, they sought recognition that they were constitutionally entitled to disclose aggregate data on the number of FISA orders they had received and the number of users affected. Two weeks later, LinkedIn joined as a fifth party to the transparency litigation.[239] Lastly, Apple and Dropbox sought – and were granted – leave to participate as *amici curiae*.[240]

[135] In addition to technology companies, the Google/Microsoft constitutional transparency litigation gained traction in the larger privacy and media communities. On July 8, 2013, a coalition of privacy organizations (collectively, the "Privacy Organizations") sought leave to participate in proceedings as *amici curiae*.[241] The Privacy Organizations included the ACLU and the Electronic Frontier Foundation,[242] who informed FISC they intended to argue that the transparency sought by Google and Microsoft "lies at the core of the constitutional protection for free expression."[243] In parallel, a coalition of leading media companies (collectively, the "Media Companies") also sought leave to participate as *amici*.[244] The Media Companies included the Associated Press, Dow Jones & Company, The New York Times Company, and Reuters America,[245] who indicated they would show that where communications providers like Google

---

constitutional free-speech rights permitted them to speak on "an issue of great importance to [] customers, shareholders, and the public," and that FISA did not prohibit disclosure of aggregate data on FISA orders. Furthermore, the companies pointed out that disclosure of aggregate data would not endanger national security.

[237] *See In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives*, No. Misc. 13-05 (F.I.S.C. filed Sept. 9, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-05%20Motion-12.pdf.

[238] *See In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives*, No. Misc. 13-06 (F.I.S.C. filed Sept. 9, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-06%20Motion-3.pdf.

[239] *See In re Motion for Declaratory Judgment that LinkedIn Corp. May Report Aggregate Data Regarding FISA Orders*, No. Misc. 13-07 (F.I.S.C. filed Sept. 17, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-07%20Motion-3.pdf.

[240] *See In re Motions to Disclose Aggregate Data Regarding FISA Orders and Directives*, (F.I.S.C. Oct. 1, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-04%20Order-11.pdf (Dropbox); *Id.* (F.I.S.C. Nov. 13, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Order-15.pdf (Apple).

[241] *In re Motion for Declaratory Judgment of Google, Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, No. Misc. 13-03 and *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, No. Misc. 13-04, (F.I.S.C. filed July 8, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-12.pdf.

[242] *Id.* at 2.

[243] *Id.*

[244] Mot. of the Reporters Committee for Freedom of the Press et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, -03, -04 (F.I.S.C. July 15, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-4.pdf.

[245] *Id.* at 2. The complete list of Media Companies comprised: (1) Reporters Committee for Freedom of the Press; (2) The Associated Press; (3) Dow Jones & Company; (4) Gannett Co.; (5) the Los Angeles Times; (6) The McClatchy Company; (7) National Public Radio; (8) The New York Times Company; (9) The New Yorker; (10)

and Microsoft "are willing speakers, the public has a heightened interest in hearing their speech."[246] FISC granted both the Privacy Organizations and the Media Companies leave to participate as *amici*.[247]

[136] This created a remarkable situation from a surveillance-oversight perspective. Seven leading technology and communications companies had challenged the constitutionality of the Department of Justice's prohibition on publishing national-security process statistics. The FISC then permitted leading Privacy Organizations, such as the Electronic Frontier Foundation, and leading Media Companies such as the New York Times to participate in the constitutional challenge. The result was a broad coalition of transparency interests litigating the constitutionality of DOJ action.

3. A Change in Policy Permits Transparency Reporting Rights

[137] The Google/Microsoft transparency litigation initially resulted in the Department of Justice changing its policy on reporting. The Department of Justice permitted two alternative approaches under which communications companies could report aggregate ranges of data on FISA orders and affected subscribers.[248] For the first time since FISA was passed in 1978,

---

The Newsweek/Daily Beast Company; (11) Reuters America LLC; (12) Tribune Company; and (13) the Washington Post.

[246] *Id.* at 2.

[247] In *re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, -03, -04 (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-3.pdf.

[248] *See* Letter dated Jan. 27, 2014 from James M. Cole, Deputy AG, DOJ, to the General Counsels of Google, Microsoft, Yahoo, Facebook, and LinkedIn, https://www.justice.gov/iso/opa/resources/422201412716042240387.pdf. The two alternative reporting approaches the parties agreed to were as follows:

> Option One. A provider may report aggregate data in the following separate categories [every six months]:
> 1. Criminal process, subject to no restrictions.
> 2. The number of NSLs [National Security Letters] received, reported in bands of 1000 starting with 0-999.
> 3. The number of customer accounts affected by NSLs, reported in bands of 1000 starting with 0-999.
> 4. The number of FISA orders for content, reported in bands of 1000 starting with 0-999.
> 5. The number of customer selectors targeted under FISA content orders, in bands of 1000 starting with 0-999.
> 6. The number of FISA orders for non-content, reported in bands of 1000 starting with 0-999.
> 7. The number of customer selectors targeted under FISA non-content orders, in bands of 1000 starting with 0-999.
>
> [. . .]
>
> Option Two. In the alternative, a provider may report on aggregate data in the following separate categories:
> 1. Criminal process, subject to no restrictions.
> 2. The total number of all national security process received, including all NSLs and FISA orders, reported as a single number in the following bands: 0-249 and thereafter in bands of 250.

companies were permitted to publicly report ranges of numbers showing "[t]he number of FISA orders for content," as well as "[t]he number of customer selectors targeted under FISA content orders"[249] – both of which had been at the center of public debate following the disclosure of the PRISM program.

[138] Notably, the Deputy Attorney General of the Department of Justice responsible for settlement negotiations expressed gratitude to Google and Microsoft for pursuing the issue of transparency reporting, stating he "appreciated the opportunity to discuss these issues with you, and [was] grateful for the time, effort, and input of your companies in reaching a result that we believe strikes an appropriate balance between the competing interests of protecting national security and furthering transparency."[250] This change in the Department of Justice's reporting policy was reached just over six months after Google and Microsoft filed their initial motions for declaratory judgment.

4. The USA FREEDOM Act Codifies Transparency Reporting Rights

[139] The USA FREEDOM Act introduced amendments to FISA that codify and expand the reporting rights first recognized through the Google/Microsoft settlement. Under amended FISA reporting provisions, recipients of FISA orders now have four statutorily-guaranteed approaches through which they can report aggregate ranges of data on orders received and the number of customers affected.[251]

---

3. The total number of customer selectors targeted under all national security process, including all NSLs and FISA orders, reported as a single number in the following bands, 0-249, and thereafter in bands of 250.

Id. at 2-3.

[249] *See id.*

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

[251] *See* 50 U.S.C. § 1874(a): A person subject to a nondisclosure requirement accompanying an order or directive under this chapter or a national security letter may, with respect to such order, directive, or national security letter, publicly report the following information using one of the following structures:

(1) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of--

(A) the number of national security letters received, reported in bands of 1000 starting with 0-999;

(B) the number of customer selectors targeted by national security letters, reported in bands of 1000 starting with 0-999;

(C) the number of orders or directives received, combined, under this chapter for contents, reported in bands of 1000 starting with 0-999;

(D) the number of customer selectors targeted under orders or directives received, combined, under this chapter for contents[1] reported in bands of 1000 starting with 0-999;

(E) the number of orders received under this chapter for noncontents, reported in bands of 1000 starting with 0-999; and

(F) the number of customer selectors targeted under orders under this chapter for noncontents, reported in bands of 1000 starting with 0-999, pursuant to--

(i) subchapter III;

(ii) subchapter IV with respect to applications described in section 1861(b)(2)(B) of this title; and

(iii) subchapter IV with respect to applications described in section 1861(b)(2)(C) of this title.

[140] Companies can report ranges of the aggregate numbers of (a) National Security Letters, (b) FISA orders or directives, or (c) non-content requests – along with the "number of customer selectors" targeted under each such request.[252] Companies may also continue to report ranges of the "total number of all national security process received" – including National Security Letters and FISA orders and directives – as well as the number of customers affected by all such requests.[253] Companies may issue compliance reports annually or semiannually, at their option.

[141] The FISC litigation and the USA FREEDOM Act's recently-enacted provisions have encouraged corporations to publish transparency reports containing granular information about the number of requests for user information. The Berkman Center for Internet and Society has developed a best practices guide for companies in detailing information in transparency reporting on US government requests for user information, including detailing content versus non-content, outcomes, user notification, and legal processes.[254] The transparency reports of most major technology companies in the US, including Facebook, Google, Apple, and Yahoo, follow these

---

(2) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of--

(A) the number of national security letters received, reported in bands of 500 starting with 0-499;

(B) the number of customer selectors targeted by national security letters, reported in bands of 500 starting with 0-499;

(C) the number of orders or directives received, combined, under this chapter for contents, reported in bands of 500 starting with 0-499;

(D) the number of customer selectors targeted under orders or directives received, combined, under this chapter for contents, reported in bands of 500 starting with 0-499;

(E) the number of orders received under this chapter for noncontents, reported in bands of 500 starting with 0-499; and

(F) the number of customer selectors targeted under orders received under this chapter for noncontents, reported in bands of 500 starting with 0-499.

(3) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply in the [sic] into separate categories of--

(A) the total number of all national security process received, including all national security letters, and orders or directives under this chapter, combined, reported in bands of 250 starting with 0-249; and

(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this chapter, combined, reported in bands of 250 starting with 0-249.

(4) An annual report that aggregates the number of orders, directives, and national security letters the person was required to comply with into separate categories of--

(A) the total number of all national security process received, including all national security letters, and orders or directives under this chapter, combined, reported in bands of 100 starting with 0-99; and

(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this chapter, combined, reported in bands of 100 starting with 0-99.

[252] *See id.* § 1874(a)(1).

[253] *See id.* § 1874(a)(4).

[254] *See* RYAN BUDISH, ET AL., NEW AMERICA, OPEN TECHNOLOGY INSTITUTE, HARV. BERKMAN CENTER FOR INTERNET & SOCIETY, *The Transparency Reporting Toolkit* (Mar. 31, 2016), https://www.newamerica.org/oti/policy-papers/the-transparency-reporting-toolkit/.

principles.[255]

IV. The FISC Will Benefit from Non-Governmental Briefing in Important Cases

[142] When FISA was enacted in 1978, the FISC's main task was to issue individual wiretap orders by applying FISA's probable cause standard to specific facts. These proceedings were *ex parte*, with the Department of Justice presenting facts to the FISC for review. After 2001, the FISC began an expanded role in overseeing entire foreign intelligence programs. These presented more complex legal issues, and there was increasing recognition that FISC judges would benefit from briefing by non-governmental parties.

[143] This section reviews newly-declassified materials showing how the FISC began to receive such briefing of its own initiative, and how FISA has been amended to ensure the FISC receives adversarial third-party briefing in significant cases. Part A briefly outlines the FISC's avenues for receiving third-party input. Part B discusses how the FISC created some opportunities for information services providers to brief the court. Part C shows how going forward, the USA FREEDOM Act has created a panel of privacy and civil liberties experts who will have access to classified information and brief the Court in important cases.

A. FISC Rules Foresee a Number of Avenues for Third-Party Participation

[144] FISA, the FISC Rules of Procedure, and FISC decisions anticipate third-party participation in FISC proceedings. Third parties can initiate proceedings, appear as defendants to governmentally-requested relief, and participate as *amici*. To initiate proceedings, FISC Rule of Procedure 6(d) permits any person to file a motion with the FISC requesting relief.[256] The relief that can be requested of the FISC is not limited; third parties have filed motions requesting actions ranging from publication of orders[257] to entry of a declaratory judgment.[258] Also, any

---

[255] *See, e.g.*, *US Transparency Report*, GOOGLE, https://www.google.com/transparencyreport/userdatarequests/US/; *US Transparency Report*, FACEBOOK, https://govtrequests.facebook.com/country/United%20States/2015-H2/; *Transparency Report*, APPLE, http://images.apple.com/legal/privacy/transparency/requests-2015-H2-en.pdf; *Transparency Report*, AT&T, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html; *Transparency Report*, YAHOO!, https://transparency.yahoo.com/government-data-requests/country/United%20States**/31/?tid=31.

[256] *See* F.I.S.C. R.P. 6(d): "A party seeking relief, other than pursuant to an application, certification, or petition permitted under the Act and these Rules, must do so by motion." Motions filed with FISC look much like motions filed with any other US federal court: they must state the relief desired, contain citations to pertinent provisions of law, and set forth attorney contact information. *See id.* R. 7(f), (h)(1). Some differences do exist between FISC motions and motions filed in other US federal courts. FISC motions must state whether the attorney representing the filing party has a security clearance, and if so, describe (a) the circumstances in which the clearance was granted, (b) the agencies that granted the clearance, and (c) the classification levels and compartments involved. *See* FISC Rule of Procedure 7(i). Additionally, motions filed with FISC must be served on the government prior to or contemporaneously with filing. *See* F.I.S.C. R.P. 8(a).

[257] For example, see my discussion of the ACLU transparency litigation in Section III(A)(2), *supra*.

[258] For an example, see the discussion of the Google/Microsoft transparency-reporting litigation in Section III(B), *supra*.

company that has been ordered to produce data via a FISC order may file a "petition for review" challenging the legality of the FISC order.[259]

[145] In addition to initiating proceedings, FISC Rules of Procedure anticipate that third parties will become defendants to adversarial litigation. If a communications provider declines to comply with a directive to produce data in response to FISC orders, the government may file a "petition to compel compliance" with the directive.[260] As will be seen below, such petitions can result in constitutional litigation requiring appellate review.[261]

[146] Lastly, FISC decisions have held that the FISC's Article III authority entails the inherent power to permit third parties to participate in proceedings as *amici curiae*.[262] While in the past participation by *amici* was limited to situations where third parties actively moved the FISC for permission to submit briefing, the USA FREEDOM Act now requires *amici* to be named in novel or significant cases.[263]

B. The FISC Has Adjudicated Substantial Adversarial Litigation

[147] This section explores a case that illustrates substantial adversarial litigation that the FISC has adjudicated. In 2007, Yahoo!, Inc. (Yahoo) challenged the constitutionality of the Protect America Act, which at the time contained amendments to FISA. Yahoo's challenge resulted in extensive briefing, two levels of review, oral argument, and two detailed opinions. It also resulted in case law holding that communications providers have standing to file constitutional challenges on behalf of their subscribers. The Yahoo litigation can be seen as a model for how significant questions of law will be tested via adversarial presentation before the FISC in future cases.

1. Background

[148] In 2007, Congress passed the Protect America Act (PAA) as an interim measure preceding the FISA Amendments Act of 2008. Section 105B of the PAA was the predecessor to the current Section 702 of FISA, which permits the NSA to acquire communications of individuals outside the US pursuant to FISC-approved targeting and minimization procedures. Relying on Section 105B, the US government served directives on Yahoo ordering it to produce communications to or from tasked selectors. Yahoo refused to comply on grounds that the directives violated the Fourth Amendment of the US Constitution. The government filed a petition to compel Yahoo's compliance, and Yahoo's constitutional challenge thus arrived before the FISC for review.

---

[259] F.I.S.C. R.P. 6(c); *see also* 50 U.S.C. § 1881a(h)(4)(A): "An electronic communication service provider receiving a directive issued pursuant to [FISA] may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition."
[260] *See* F.I.S.C. R.P. 22.
[261] *See* Section IV(B) *infra*.
[262] *See In re Application of the F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 14-01 (F.I.S.C. Mar. 21, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR%2014-01%20Opinion-3.pdf.
[263] *See* Section IV(C) *infra*.

2. Proceedings before the FISC

[149] Declassified materials[264] show that the FISC afforded the Yahoo litigation the degree of attention that significant constitutional questions generally receive in US federal courts. The FISC issued orders granting Yahoo's counsel access to classified information to litigate the matter.[265] The FISC received extensive briefing,[266] and ordered further submissions on issues it deemed important.[267] The Court required the parties to clarify technical issues.[268] Then, the FISC issued a 98-page opinion containing a thorough analysis of Yahoo's challenge.[269]

[150] In its opinion, the FISC held as a matter of constitutional law that communications providers like Yahoo have standing to challenge the constitutionality of US surveillance statutes on behalf of their subscribers. The FISC stated that service-provider standing rights were

---

[264] Many of the pleadings, orders, and other filings from the Yahoo litigation can be found on the DNI's website, *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statement by the ODNI and the US DOJ on the Declassification of Documents Related to the PAA Litigation* (Sept. 11, 2014), https://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1109-statement-by-the-office-of-the-director-of-national-intelligence-and-the-u-s-department-of-justice-on-the-declassification-of-documents-related-to-the-protect-america-act-litigation, as well as on a website maintained by the Los Angeles Times devoted to the Yahoo case, *see* Lauren Raab *et al*., *Search the Yahoo FISA Case Documents*, L.A. TIMES, http://documents.latimes.com/yahoo-fisa-case/.

[265] *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 at 2 (F.I.S.C. Dec. 28, 2007), https://www.dni.gov/files/documents/0909/Order%20Establishing%20Procedures%2020071228.pdf. Yahoo's counsel possessed a top-secret security clearance. *Id.*

[266] FISC received two initial rounds of briefing: (a) the government's motion to compel and Yahoo's memorandum in opposition, along with (b) a supplemental memorandum of law from the government, followed by Yahoo's response. *See* Government's Mot. to Compel, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Nov. 21, 2007), https://www.dni.gov/files/documents/0909/Government%20Motion%2020071121.pdf; Yahoo's Resp. to Government's Mot. to Compel, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Nov. 30, 2007), https://www.dni.gov/files/documents/0909/Yahoo%20Opposition%20Memo%2020071130.pdf.

[267] The FISC (1) ordered the government to submit additional briefing responding to Yahoo's contention that Yahoo had standing to bring a constitutional challenge based on alleged violations of the privacy rights of its subscribers; (2) ordered additional briefing on the question of whether the PAA directives issued to Yahoo were consistent with privacy rights; and (3) ordered briefing as to whether the PAA permitted the government to amend the PAA directives to Yahoo during ongoing litigation. *See In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Feb. 6, 2008), https://www.dni.gov/files/documents/0909/Order%2020080206.pdf; *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01, 3-4, 43 (F.I.S.C. Apr. 25, 2008), https://www.dni.gov/files/documents/0909/Memorandum%20Opinion%2020080425.pdf.

[268] FISC requested clarification on "what Yahoo has been directed to provide the government" and "the manner in which such production is to be effectuated." *See In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01, 1 (F.I.S.C. Jan. 4, 2008), https://www.dni.gov/files/documents/0909/Order%20Directing%20Filing%2020080104.pdf. As a result, the FBI's Investigation Data Acquisition/Intercept Section filed a declaration describing the PAA directives and surveillance techniques at issue, while Yahoo's General Counsel as well as the manager of Yahoo's Legal Department Compliance Team responded via affidavit. *See* FISC Docket 105B(g) 07-01 Entries 34 and 37, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, https://www.dni.gov/files/documents/0909/Docket%20Entry%20Sheet.pdf.

[269] *See In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Apr. 25, 2008), https://www.dni.gov/files/documents/0909/Memorandum%20Opinion%2020080425.pdf.

"critically important" within "the context of a statute that authorizes the government to acquire the contents of communications" without the targeted person's knowledge.[270] On the merits, the FISC found that the PAA ensured that reasonable safeguards were in place to protect privacy, and thus held that the directives issued to Yahoo were constitutional.

3. Proceedings before the FISCR

[151] Yahoo appealed the FISC's ruling to the Foreign Intelligence Surveillance Court of Review (FISCR).[271] The FISCR afforded Yahoo's challenge the treatment significant constitutional questions generally receive before US appellate courts. The FISCR received thorough briefing;[272] heard *inter partes* oral argument from the government and Yahoo;[273] and received additional post-argument briefing from both parties.[274] The FISCR then issued a 35-page opinion analyzing existing authorities and resolving Yahoo's challenge.[275]

[152] Like the FISC, the FISCR held that Yahoo had standing to bring a constitutional challenge to US surveillance statutes to protect customer privacy rights.[276] The FISCR noted

---

[270] *Id.* at 45.

[271] FISA permits communications providers whose challenges to surveillance orders are denied by the FISC to appeal the FISC's decision to the FISCR. *See* 50 U.S.C. § 1881a(h)(6) ("[A]n electronic communication service provider receiving a directive issued pursuant to [FISA] may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision [of the FISC adjudicating the provider's challenge]."). The PAA contained a similar appeal provision.

[272] Yahoo filed an initial appellate brief comprising 74 pages. Brief of Appellant Yahoo!, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed May 29, 2008), https://www.dni.gov/files/documents/0909/Yahoo%20Brief%2020080529.pdf. The government responded with a 68-page opposition brief. Ex-Parte Brief for Respondent, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed June 5, 2008), https://www.dni.gov/files/documents/0909/Government%20Ex%20Parte%2020080605.pdf. Yahoo then filed a 35-page reply. Reply Brief of Appellant Yahoo! *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed June 9, 2008), http://www.documentcloud.org/documents/1300533-3-yahoo-reply-brief.html.

[273] *See* Transcript of June 19, 2008 Oral Argument, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. June 19, 2008), https://www.dni.gov/files/documents/1118/19%20June%202008%20FISCR%20PAA%20Hearing%20Transcript%20-%20Declassified%20FINAL.pdf. Oral argument lasted 80 minutes, which is 20 minutes longer than the US Supreme Court generally permits parties to argue a constitutional case.

[274] Following oral argument, the government filed a 42-page supplemental brief. Ex-Parte Supplemental Brief for Respondent, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed June 26, 2008), https://www.dni.gov/files/documents/0909/Government%20Supplemental%20Brief%2020080626.pdf. Yahoo filed a response. Motion for Leave to File Reply to the Government's Supplemental Briefing *Instanter, In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (filed June 30, 2008), https://www.dni.gov/files/documents/0909/Yahoo%20Motion%2020080630.pdf; and the government followed with a final reply brief. Motion for Leave to File a Supplementary Reply Brief, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (filed July 3, 2008), https://www.dni.gov/files/documents/0909/Government%20Motion%2020080703.pdf.

[275] *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C.R. Aug. 22, 2008), https://www.dni.gov/files/documents/0909/FISC%20Merits%20Opinion%2020080822.pdf.

[276] *Id.* at 9-11.

that FISA permitted service providers to "challenge the legality" of directives they received, and that this language was "broad enough to permit a service provider to bring a constitutional challenge."[277] On the merits, the FISCR held that the PAA contained sufficient privacy-protecting procedures over NSA surveillance to render it constitutional.[278]

4. Conclusion

[153] The FISC's adjudication of Yahoo's PAA challenge illustrates the capability for adversarial litigation that the FISC has offered. The Yahoo litigation featured (1) extensive briefing; (2) two levels of review; (3) adversarial presentation of argument; (4) access by non-government counsel to classified information; and (5) adjudication on constitutional merits. This reflects the kind of review that privacy advocates have requested be instituted within surveillance oversight bodies for significant legal questions.

C. Going Forward, the FISC will Benefit from Third-Party Input in Important Cases

[154] The Yahoo litigation can be seen as a template for how the FISC will approach significant questions of law in the future. The USA FREEDOM Act now requires the FISC to appoint *amici curiae* to submit adversarial briefing on novel or significant issues of law. Recently declassified cases show that the *amicus* mechanism is already being used in surveillance approval and oversight.

[155] The USA FREEDOM Act mandated the creation of a panel of independent experts to serve as *amici curiae* to the FISC on important cases. Going forward, the FISC must appoint an *amicus curiae* in any matter that, in the court's judgement, "presents a novel or significant interpretation of the law."[279] The duty to appoint an *amicus* applies in any FISC proceeding, including NSA applications for surveillance authorizations, requests for any other order, or applications for appellate review.[280] The FISC retains some discretion on when to appoint an amicus curiae, but the clear intent of the statute is that independent lawyers will participate before the FISC in important cases.

[156] The first criterion for selection to the FISC's *amicus* panel is "expertise in privacy and civil liberties."[281] The presiding judges of the FISC and the FISCR jointly appoint the panel of attorneys, and the FISC selects an *amicus* from the panel in appropriate cases.[282] As of March 31, 2016, six well-regarded privacy experts have been approved as FISC *amici*, including a professor and lawyers who have been involved in foreign-intelligence matters through prior government service or in private practice.[283]

---

[277] *Id.* at 10-11.
[278] *Id.* at 12-33.
[279] 50 U.S.C. § 1803(i)(2)(A).
[280] *Id.*
[281] *Id.* § 1803(i)(3)(A).
[282] *Id.* § 1803(i)(1).
[283] *See* U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Amici Curiae*, http://www.fisc.uscourts.gov/amici-curiae. As of the date of this Report, the current panel of FISC *amici* consists of: (1) Jonathan Cedarbaum (partner,

[157] As to the duty of *amici* when appointed to a case, to the extent privacy or constitutional issues are relevant, a FISC-appointed *amicus* must present "legal arguments that advance the protection of individual privacy and civil liberties."[284] To perform their duties, FISC *amici* are security-cleared to permit them to access classified information.[285] *Amici* also have access to any "legal precedent, application, certification, petition, motion, or such other materials" the FISC deems relevant.[286]

[158] In addition to proceedings before the FISC, the USA FREEDOM Act ensures appellate review of significant FISC rulings. The FISC must now certify decisions to FISCR for appellate review when, in the FISC's opinion, its decision potentially creates issues of uniformity in federal law.[287] *Amici* may be appointed to participate in appellate proceedings as well.

[159] Recently-declassified opinions show that the FISC and the FISCR have appointed *amici* in cases presenting significant legal questions. The FISCR recently appointed an *amicus* to present adversarial briefing on the issue of whether Pen Register/Trap-and-Trace surveillance should be permitted to acquire information referred to as "post-cut-through digits."[288]

[160] Moreover, the FISC appointed an *amicus* to assist it in reviewing a government request to conduct surveillance. During its evaluation of the government's 2015 certification to reauthorize Section 702 programs, the FISC appointed an *amicus* to argue whether the government's proposed minimization measures were consistent with the Fourth Amendment.[289] The FISC-appointed expert submitted briefing to the FISC and participated in oral argument.[290] In its opinion authorizing the programs, the FISC noted it "wished to thank" the *amicus* "for her exemplary work in this matter," and that her presentations "were extremely informative to the Court's consideration of this matter."[291]

WilmerHale); (2) John Cline (Law Office of John D. Cline); (3) Laura Donohue (professor, Georgetown University School of Law); (4) Amy Jeffress (partner, Arnold & Porter); (5) Marc Zwillinger (managing member, ZwillGen PLLC); and (6) David Kris (general counsel, Intellectual Ventures).

[284] 50 U.S.C. § 1804(i)(4)(A).

[285] *Id.* § 1803(i)(3)(B).

[286] *Id.* § 1804(i)(6)(A).

[287] *See id.* § 1803(j).

[288] *See In re Certified Question of Law*, No. FISCR 16-01 (F.I.S.C.R. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf. For a more detailed discussion of PR/TT surveillance and post-cut-through digits, see section I(B)(5) *supra*.

[289] *See [Caption Redacted]*, [Case no. redacted] at 6 (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

[290] *Id.* at 6-7.

[291] *Id.* at 6 n.6.

CHAPTER 6:

COMPARATIVE SURVEILLANCE SAFEGUARDS DEVELOPED BY OXFORD RESEARCH TEAM

[1] To assist in the comparison of EU and US national security surveillance practices, this Chapter applies criteria for national security surveillance laws developed by a team led by noted European privacy expert Professor Ian Brown of Oxford University.[1]

[2] The Oxford team developed a framework to analyze the categories of reform called for in democratic societies in the wake of revelations of large-scale electronic surveillance by the US and EU Member States. The Oxford team based its framework on what it called four "prominent" proposals for surveillance reforms:[2]

1. The International Principles on the Application of Human Rights to Communications Surveillance, which listed 13 "necessary and proportionate" principles to codify human rights obligations in the field of foreign surveillance.[3]

2. The report of the European Parliament Civil Liberties (LIBE) Committee concerning the Snowden revelations.[4]

3. Principles for surveillance reform that were endorsed by leading technology companies including AOL, Apple, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo.[5]

4. The recommendations of President Obama's Review Group on Intelligence and Communications Technology, on which I served.[6]

[3] This Chapter applies the 11 categories of safeguards derived by the Oxford team from these four sources. For each category, I cite the applicable guidance from the four reform proposals,

---

[1] Professor of Information Security and Privacy at the Oxford Internet Institute. His research is focused on surveillance, privacy-enhancing technologies, and Internet regulation. He is an ACM Distinguished Scientist and BCS Chartered Fellow, and a member of the Information Commissioner's Technology Reference Panel. *See* IAN BROWN, MORTON H. HALPERIN, BEN HAYES, BEN SCOTT, AND MATHIAS VERMEULEN, TOWARDS MULTILATERAL STANDARDS FOR SURVEILLANCE REFORM, https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf. The discussion in this chapter is based on my review of the paper, and I have not been in contact with Professor Brown or his team in the preparation of my testimony.

[2] *Id.* at 18-24.

[3] NECESSARY AND PROPORTIONATE, *July 2013 version: International Principles on the Application of Human Rights to Communications Surveillance* (July 10, 2013), https://necessaryandproportionate.org/text/2013/07/10 [hereinafter *International Principles*].

[4] European Parliament Comm. on Civil Liberties, Justice and Home Affairs, *Rep. on the US NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, A7-0139/2014 (Feb. 21, 2014), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN [hereinafter *LIBE Report*].

[5] REFORM GOV'T SURVEILLANCE, *Global Government Surveillance Reform: The Principles* (Dec. 9, 2013), https://www.reformgovernmentsurveillance.com/ [hereinafter *Company Principles*].

[6] PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY (2014), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter REVIEW GROUP REPORT].

listed above. I cite the Review Group recommendations and US reforms to date for that category. I then cite reviews of European practices by EU commentators since the Snowden disclosures.

[4] I believe this approach provides a systematic and relatively objective way to assess and reconcile current EU and US safeguards. As discussed further in the conclusion, my own view is similar to that of the Oxford team: that the US, after the reforms that occurred in the wake of the Snowden revelations, is the new "benchmark" for transparent principles, procedures, and oversight for national security surveillance.[7]

I. Categories for Comparison

[5] After grouping the reform recommendations into 11 categories, the Oxford team summarized each of the reform proposals relative to the respective category: (1) mandatory retention of metadata; (2) bulk collection; (3) data mining; (4) judicial control; (5) disclosure of legal authorities; (6) rights of subjects of foreign surveillance; (7) notification of data subjects; (8) data minimization; (9) onward transmission/purpose limitation; (10) transparency; and (11) oversight. For each of the categories developed by the Oxford team, I provide: (a) the approach recommended by the Review Group and subsequent US reforms; and (b) review of European practices by EU commentators since the Snowden disclosures.

1. Mandatory Retention of Metadata

[6] In the category of mandatory retention of metadata, the Oxford team identified the following reform approaches:

> *The International Principles*: The reforms focused on the idea that *a priori* data collection and retention should not be required of service providers.[8]
>
> *The LIBE Report*: The document stated that data retention was incompatible with Article 52(1) of the Charter of Fundamental Rights of the European Union.[9]
>
> *The principles of technology companies:* The companies advocated for limitations on the government's ability to compel service providers to disclose user data.[10]
>
> *The Review Group:* For foreign intelligence purposes, it recommended the US government introduce a system in which metadata is no longer held by the government, but is held by private providers or by a private third party, with access to such data permitted only with an order from the Foreign Intelligence Surveillance Court (FISC).[11]

[7] Brown et al., *supra* note 1, at 19.
[8] *See International Principles*, *supra* note 3, at "Integrity of communications systems"; Brown et al., *supra* note 1, at 20.
[9] *LIBE Report*, *supra* note 4, at Preamble; *see* Brown et al., *supra* note 1, at 20.
[10] *Company Principles*, *supra* note 5, para. 1; *see* Brown et al., *supra* note 1, at 20.
[11] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 5; *see* Brown et al., *supra* note 1, at 20.

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[7] *Review Group Recommendation 5:* "We recommend that legislation should be enacted that terminates the storage of bulk telephony meta-data by the government under section 215, and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party. Access to such data should be permitted only with a section 215 order from the Foreign Intelligence Surveillance Court."[12] This recommendation was based, in large part, on the Review Group's finding "that the information contributed to terrorist investigations by the use of Section 215 telephony metadata was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional Section 215 orders."[13]

[8] *Reforms since 2013:* The USA FREEDOM Act ended the bulk collection practice under Section 215 for collection of "tangible things" (including phone records).[14] There is no mandatory data retention in the US for Internet records. Telephone records that are needed for billing purposes are retained for 18 months.[15]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[9] *Review by Professor Federico Fabrinni:* Data retention requirements have been a prominent feature of European debates about how to achieve privacy protection consistent with law enforcement and national security goals. In 2006, the EU promulgated a Data Retention Directive,[16] which required publicly available electronic communications services to retain records for an extended period of time, for purposes of fighting serious crime. For instance, for email and other electronic communications, the communications services were required to retain "the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication."[17] In the *Digital Rights Ireland* case, the European Court of Justice struck down that Directive due to privacy concerns related to excessive access to the retained data and lack of assurances that the records would be destroyed at the end of the retention

---

[12] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 5.
[13] *Id.*
[14] 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, § 103 (2015), https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf.
[15] 47 C.F.R. § 42.6. The telephone retention rule is discussed in REVIEW GROUP REPORT, *supra* note 6, at 119 n. 118.
[16] EU Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006 O.J. (L 105), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF [hereafter "Data Retention Directive"].
[17] *Id.*, Art. 5(1)(b).

period.[18] In the wake of that judgment, a number of EU Member States have reinstated modified data retention requirements for telephone and Internet communications.[19]

[10] Data retention is an ongoing issue, with cases pending before the European Court of Justice.[20]

2. Bulk Collection

[11] In the category of bulk collection, the Oxford team analyzed the following reform approaches:

> *The International Principles:* The group advocated for a prohibition on bulk collection.[21]
>
> *The LIBE Report:* The report advocated for a prohibition on bulk collection.[22]
>
> *The principles of technology companies:* The companies advocated for a prohibition on bulk collection.[23]
>
> *The Review Group:* We recommended an end to collection and storage of all mass undigested, non-public personal information. We also suggested that any program involving collection or storage of such data should be narrowly tailored to serve an important government interest and called for agencies to examine the feasibility of creating software allowing targeted information acquisition.[24]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[12] *Review Group Recommendation 4:* "We recommend that, as a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest."

---

[18] *See* Case C-293/12, *Digital Rights Ireland v. Minister of Commc'ns*, 2014 E.C.R. I-238, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.

[19] *See* Federico Fabrinni, *Human Rights in the Digital Age: The European Court of Justice Ruling in Digital Rights Ireland and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUM. RIGHTS J., 73-74, 88 (2015), http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf.

[20] *Op. of the Advocate General* in Joined Cases C-203/15, *Tele2 Sverige AB v. Post-och telestyrelsen* and C-698/15, *Sec. of State for Home Dep't v. Watson* (2016), http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=EN&mode=req&occ=first.

[21] *International Principles*, *supra* note 3, at "Proportionality" and "Competent Judicial Authority"; *see* Brown et al., *supra* note 1, at 20.

[22] *LIBE Report*, *supra* note 4, at paras. 17, 21; *see* Brown et al., *supra* note 1, at 20.

[23] *Company Principles*, *supra* note 5, para. 1; *see* Brown, et al., at 20.

[24] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 4, 20; *see* Brown et al., *supra* note 1, at 20.

[13] *Review Group Recommendation 20:* "We recommend that the US Government should examine the feasibility of creating software that would allow the [NSA] and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection."[25]

[14] *Reforms since 2013:* The USA FREEDOM Act prohibited bulk collection under three authorities: (1) Section 215, for collection of "tangible things" (including phone records);[26] (2) Foreign Intelligence Surveillance Act (FISA) pen register and trap and trace authorities (to/from information about communications);[27] and (3) National Security Letters (phone, financial, and credit history records).[28]

[15] In addition, Section 2 of Presidential Policy Directive 28 (PPD-28) creates new limitations on the use of signals intelligence for the collection of communications that, in the initial stages, targets not an individual but a large flow of data. More specifically, PPD-28 limits the use of signals intelligence for "authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants," such as email or other selectors.[29] PPD-28 announces purpose limitations – when the US collects large quantities of nonpublicly available information, 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 US and its interests;
(2) Threats to the US and its interests from terrorism;
(3) Threats to the US 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;
(6) Transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.[30]

If this list is updated, it will be "made publicly available to the maximum extent feasible."[31]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[16] *Review in the 2013 Report to the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs*: According to the Report, the "practice of so-called 'upstreaming' –

[25] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 20.
[26] USA FREEDOM Act § 103.
[27] *Id.* at § 201.
[28] *Id.* at § 501.
[29] THE WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, Presidential Policy Directive, Signals Intelligence Activities, PPD-28, § 2 (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28]. PPD-28 further provides that the "[t]he limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection." *Id.*
[30] *Id.*
[31] *Id.*

tapping directly into the communications infrastructure as a means to intercept data – appears to be a relatively widespread feature of surveillance by several EU Member States, namely the UK, Sweden, France, and Germany."[32] The UK's Tempora program is engaged in routine interception of approximately 200 undersea cables that transmit Internet data into and out of the British Isles.[33] In Sweden, the government monitors cable-bound communications into and out of Sweden, including telephone calls, text messages, and emails.[34] The French program for large-scale surveillance is reported to collect, process, and store petabytes of data collected from at least 20 interception points comprised of both satellite stations and tapping fiber-optic submarine cables outside the country.[35] In Germany, the program for large-scale surveillance directly connects to digital traffic nodes through which foreign communications flows. German intelligence agencies are legally allowed to search up to 20% of the communications having a foreign element for national security reasons.[36] The Report concluded: "Surveillance programs in EU member states are incompatible with minimum democratic rule of law standards derived from the EU Charter of Fundamental Rights and the European Convention on Human Rights, and are in turn essential components of their national constitutional traditions."[37]

3. Data Mining

[17] In the category of data mining, the Oxford team identified the following reform approaches:

The International Principles: The issue was not addressed.[38]

The LIBE Report: The issue was not addressed.[39]

The principles of technology companies: The issue was not addressed.[40]

The Review Group: We recommended Civil Liberties Impact Assessments to ensure that any big data and data-mining programs are statistically reliable, cost-effective, and protective of privacy.[41]

---

[32] Didier Bigo et al., European Parliament Comm. on Civil Liberties, Justice and Home Affairs, *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law* (2013), at 20, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.
[33] *Id.* at 50-51.
[34] *Id.* at 58-60.
[35] *Id.* at 63-64.
[36] *Id.* at 73-74.
[37] *Id.* at 27.
[38] The category is not addressed in the *International Principles*; *see* Brown et al., *supra* note 1, at 21.
[39] The category is not addressed in the *LIBE Report*; *see* Brown et al., *supra* note 1, at 21.
[40] The category is not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 21.
[41] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 35, 36; *see* Brown et al., *supra* note 1, at 21.

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[18] *Review Group Recommendation 35:* "We recommend that for big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are statistically reliable, cost-effective, and protective of privacy and civil liberties."[42]

[19] *Review Group Recommendation 36:* "We recommend that for future developments in communications technology, the US should create program-by-program reviews informed by expert technologists, to assess and respond to emerging privacy and civil liberties issues, through the Civil Liberties and Privacy Protection Board or other agencies."[43]

[20] *Reforms since 2013:* Since 2013, the Privacy and Civil Liberties Oversight Board (PCLOB) has released detailed reports on the Section 215[44] and Section 702[45] surveillance programs, making numerous recommendations. Its central recommendations on the Section 215 telephone metadata program were enacted in the USA FREEDOM Act. Overall, the PCLOB made 22 recommendations in its Sections 215 and 702 reports, and virtually all have been accepted and either implemented or are in the process of being implemented.[46]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[21] *Review by the Report prepared for the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs:* According to the Report, the scale of the big data collected from Upstream interception requires establishing techniques, methods, and infrastructure to filter the enormous data flows. Large-scale electronic surveillance suggests data extraction, data comparison, data retention, and the use of numerous databases. The Report found it unfortunate that concrete and detailed information on how data is collected in these Upstream programs by Member States is unavailable, although hints were uncovered in reports and expert statements.[47]

[22] The Report discussed the so-called "Massive Volume Reduction" employed by the UK's Government Communications Headquarters (GCHQ) to remove approximately 30% of the data that is deemed less intelligence relevant. It noted that the lack of details on this program or the others used by EU Member States "leaves an important gap in our understanding of the practices that intelligence services are engaging in to exploit the bulk data collected. These details would

---

[42] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 35.
[43] *Id.* at Recommendation 36.
[44] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (January 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.
[45] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.
[46] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, RECOMMENDATIONS ASSESSMENT REPORT (February 5, 2016), https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf.
[47] Bigo et. al, *supra* note 32, at 23.

be critical to determine operational legitimacy and interaction with national frameworks regulating surveillance."[48]

4. Judicial Control

[23] In the category of judicial control, the Oxford team identified the following reform approaches:

> *The International Principles:* The group looked to an independent, impartial, and competent authority capable of reviewing to determine whether less invasive techniques have been considered.[49]
>
> *The LIBE Report:* The report asserted that principles of legality, necessity, proportionality, due process, and transparency – consistent with the European Convention on Human Rights – should be adhered to, with strict limits on the duration and scope of the surveillance.[50]
>
> *The principles of technology companies:* The companies advocated for independent reviewing court with an adversarial process.[51]
>
> *The Review Group:* In addition to existing judicial control under the Foreign Intelligence Surveillance Court, we recommended the creation of the position of Public Interest Advocate to represent privacy and civil liberties interests before FISC.[52]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[24] *Review Group Recommendation 28:* "We recommend that:

> 1. Congress should create the position of Public Interest Advocate to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court;
> 2. the Foreign Intelligence Surveillance Court should have greater technological expertise available to the judges;
> 3. the transparency of the Foreign Intelligence Surveillance Court's decisions should be increased, including by instituting declassification reviews that comply with existing standards; and

---

[48] *Id.*
[49] *International Principles*, *supra* note 3, at "Proportionality" and "Competent judicial authority"; *see* Brown et al., *supra* note 1, at 21.
[50] *LIBE Report*, *supra* note 4, at paras. 22, 77; *see* Brown et al., *supra* note 1, at 21.
[51] *Company Principles*, *supra* note 5, para. 2; *see* Brown et al., *supra* note 1, at 21.
[52] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 12 and 28; *see* Brown et al., *supra* note 1, at 21.

4. Congress should change the process by which judges are appointed to the Foreign Intelligence Surveillance Court, with the appointment power divided among the Supreme Court Justices."[53]

[25] *Reforms since 2013:* Consistent with the Review Group recommendation, the USA FREEDOM Act authorized the creation of a group of independent experts, called "*amici curiae*" (friends of the Court), to brief the Foreign Intelligence Surveillance Court (FISC) on important cases.[54] The law instructs the FISC to appoint an *amicus curiae* for a matter that, in the opinion of the court, "presents a novel or significant interpretation of the law."[55] The court retains discretion on when to appoint an *amicus curiae*, but the clear intent of the statute is that independent lawyers with security clearances shall participate before the FISC in important cases.

[26] This reform provides the opportunity for independent views to be heard by the FISC in important cases, so that the assertions of government officials can be carefully tested before the judge. The first statutory criterion for selection is "expertise in privacy and civil liberties."[56] The FISC has named six expert lawyers, including a professor and lawyers who have been involved in these matters either in prior government service or in private practice.[57]

[27] The USA FREEDOM Act provides that an *amicus* may be appointed for proceedings in the Foreign Intelligence Surveillance Court of Review (FISCR), under the same provision as the *amicus* is appointed for the FISC.[58] The statute also makes a provision for the appointment of an *amicus* in the event that a case is appealed from the FISCR to the United States Supreme Court.[59]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[28] *Review by the Oxford team:* The Oxford team noted the Reform Group proposal for adversarial counsel in the FISC. The Oxford team lamented that many European states do not have a clear legal process in which such privacy advocates could participate.[60]

[29] *Review by the European Union Agency for Fundamental Rights:* According to the report, only France, Germany, the Netherlands, Sweden, and the UK among the Member States have detailed public laws related to the collection of signals intelligence.[61] The EU Agency for

---

[53] *Id.*, at Recommendation 28.
[54] USA FREEDOM Act § 401.
[55] *Id.*
[56] *Id.*
[57] *See* U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Amici Curiae*, http://www.fisc.uscourts.gov/amici-curiae. For a recent report on how one such *amicus curiae* case has worked in practice, *see* Tim Cushing, *FISA Court's Appointed Advocated Not Allowing Government's 'National Security' Assertions To Go Unchallenged*, TECHDIRT.COM (Dec. 11, 2015), https://www.techdirt.com/articles/20151210/08175733048/fisa-courts-appointed-advocate-not-allowing-governments-national-security-assertions-to-go-unchallenged.shtml.
[58] USA FREEDOM Act § 401; 50 U.S.C. § 1803.
[59] *Id.*
[60] Brown et al., *supra* note 1, at 30-31.
[61] 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 AGENCY FOR FUNDAMENTAL RIGHTS REPORT], at 54.

Fundamental Rights found that none of these Member States had judicial approval of signals intelligence. Their report noted that Germany and Sweden each have an expert body in charge of authorizing signals intelligence.[62]

5. Disclosure of Legal Authorities

[30] In the category of disclosure of legal authorities, the Oxford team identified the following reform approaches:

> *The International Principles:* The group focused on notification issues that are discussed below. [63]
>
> *The LIBE report:* The report put forth the idea that secret courts violate the rule of law.[64]
>
> *The principles of the technology companies*: The companies advocated for disclosure of important rulings, in a timely manner, to ensure the courts are accountable to the public.[65]
>
> *The Review Group*: The Review Group made multiple recommendations supporting greater transparency in various respects, but did not make a specific recommendation concerning publication of legal rulings.[66]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[31] *Reforms since 2013:* Prior to 2013, the statutory provisions in the Foreign Intelligence Surveillance Act and other statutes relating to foreign intelligence were publicly available. The USA FREEDOM Act added a new provision concerning transparency of the law applying to foreign intelligence cases. Going forward, orders of the Foreign Intelligence Surveillance Court (FISC) that involve substantial interpretations of law must either be declassified or summarized and then made publicly available on the Internet.[67] This new statutory provision directly addresses the risk of secret law.

[32] Since 2013, the US administration has reviewed FISC opinions in order to declassify to the extent consistent with national security, resulting in the numerous disclosures discussed in Chapter 5 on the activities of the FISC. The Office of the Director of National Intelligence maintains a website, accessible to the public, which contains declassified opinions of FISC and its reviewing

---

In this type of collection, selectors are later applied to the data to draw out information relevant to intelligence work.

[62] *Id.*, at 54-55.

[63] *International Principles*, *supra* note 3, at "User Notification"; *see* Brown et al., *supra* note 1, at 21.

[64] *LIBE Report*, *supra* note 4, at para.14; *see* Brown et al., *supra* note 1, at 21.

[65] *Company Principles*, *supra* note 5, para. 2; *see* Brown et al., *supra* note 1, at 21.

[66] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 7, 8; *see* Brown et al., *supra* note 1, at 21-22.

[67] 50 U.S.C. § 1872(b).

body, the Foreign Intelligence Court of Review.[68] This website is called "IC on the Record" and is located at https://icontherecord.tumblr.com/.

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[33] *Review by the Council of Europe's Commissioner of Human Rights*: The report found: "In many Council of Europe members states, bulk untargeted surveillance by security services is either not regulated by any publicly available law or regulated in such a nebulous way that the law provides few restraints and little clarity on these measures. This is problematic from a human rights perspective because it makes it difficult for individuals and organizations to understand the legal basis and reasons for which their communications may be intercepted, or to challenge such surveillance as being unlawful."[69]

[34] *Review by Dr. Christina Casagran*: To the extent that public laws exist, intelligence services in the EU are only regulated at the national level. There are no EU-level laws regulating the information processed by these bodies.[70] "As a result, EU data protection rules can be circumvented via intelligence services." [71]

[35] *Review by the Oxford team:* The team concluded that, in contrast to the clear and specific rules in the US, "many of the comparative legal frameworks in European states appear to give foreign and military agencies 'carte blanche'" to engage in foreign intelligence surveillance.[72]

6. Rights of Subjects of Foreign Surveillance

[36] In the category of rights of subjects of foreign surveillance, the Oxford team discussed the following reform approaches:

> *The International Principles:* The group advocated for individuals having access to a fair and public hearing within a reasonable time by an independent tribunal, except in cases of emergency where there would be imminent risk of danger to human life.[73]

---

[68] Any additional appeals would be taken to United States Supreme Court.

[69] Council of Europe Commissioner for Human Rights, *Issue Paper: Democratic and effective oversight of national security services* (2015), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770, at 23.

[70] CRISTINA BLASI CASAGRAN, GLOBAL DATA PROTECTION IN THE FIELD OF LAW ENFORCEMENT: AN EU PERSPECTIVE 188 (2017).

[71] *Id.*

[72] Brown et al., *supra* note 1, at 9; *see also* CASAGRAN, *supra* note 87, at 187 ("It can be concluded that intelligence services in Member States often have a *carte blanche* to collect and process information and turn it into intelligence. Data collected does not only belong to EU citizens under suspicion or linked to criminal groups, but it also includes data from innocent individuals.").

[73] *International Principles*, *supra* note 3, at "Due Process"; *see* Brown et al., *supra* note 1, at 22.

The LIBE report: The report called for the US to amend legislation to recognize the privacy of EU citizens, to provide judicial redress, and to put the rights of EU citizens on an equal footing with those of US citizens.[74]

The principles of the technology companies: The companies did not address this issue.[75]

The Review Group: We recommended applying the 1974 Privacy Act[76] to both US persons and non-US persons and exploring arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens with a small number of closely allied governments.[77]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[37] *Review Group Recommendations 14:* "We recommend that, in the absence of a specific and compelling showing, the US Government should follow the model of the Department of Homeland Security, and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons."[78]

[38] *Reforms since 2013:* In February 2016, the US enacted the Judicial Redress Act extending privacy protections and remedies available under the Privacy Act to qualifying non-US individuals of covered countries. These protections generally include rights to review, copy, and request amendments to covered records maintained by designated federal agencies in the US.[79]

[39] In 2014, President Obama announced Presidential Policy Directive 28 (PPD-28), granting significant further protections to non-US citizens. PPD-28 states that – regardless of nationality – "all persons have legitimate privacy interests in the handling of their personal information," and it mandates that US intelligence agencies make privacy integral to signals intelligence planning.[80] Specifically, PPD-28 requires agencies to prioritize alternative sources of information – such as diplomatic sources – over signals intelligence.[81] Where surveillance is used, it must be "as tailored as feasible," proceeding via selectors whenever practicable.[82] Bulk collection cannot be used except to detect and counter serious threats, such as terrorism, espionage, or nuclear proliferation.[83] The European Commission found that PPD-28's protections, which apply equally to US and non-

---

[74] *LIBE Report*, *supra* note 4, at para. 30; *see* Brown et al., *supra* note 1, at 22.
[75] The category is not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 22.
[76] The Privacy Act regulates the US government's use of computerized databases of information, imposing restrictions on each federal agency's collection, use, or disclosure of personal information. 5 U.S.C. § 552a.
[77] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 14, 21; *see* Brown et al., *supra* note 1, at 22.
[78] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 14.
[79] *See generally* The Judicial Redress Act of 2016, Pub. L. No. 114-126, https://www.congress.gov/bill/114th-congress/house-bill/1428/text. For a more detailed discussion of the Judicial Redress Act, *see* Chapter 7, Section I(A)(1).
[80] Chapter 3, Section IV(B) contains a detailed discussion of the significant safeguards instituted by PPD-28. *See also* PPD-28, *supra* note 29.
[81] *See id.* § 1(d).
[82] *See id.*
[83] *See id.* § 2.

US persons, embody "the essence of the principles of necessity and proportionality."[84]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[40] *Review by Oxford team:* In EU Member States, the collection of electronic communications from outside the borders of the country is authorized for a variety of purposes. EU Member States have given themselves greater flexibility to do surveillance outside of their borders than within. For example, the UK's surveillance targets communications of non-UK residents, and the Swedish program is focused on foreign communication. Broadly speaking, the purposes for foreign surveillance in EU Member States relate to national security, external military threats, the prevention and detection of serious crimes (including terrorism), and a Member State's policy or economic interests.[85]

[41] *Review by Venice Commission:* The Venice Commission expressed its concern for a distinction being made between citizens and residents, on the one hand, and non-citizens and non-residents, on the other hand, when applying standards for targeting individuals and retaining data collected by surveillance measures. The Commission specifically focused on the US and Germany, whose safeguards legislation it stated does not apply to non-citizens and non-residents.[86]

7. Notification of Data Subjects

[42] In the category of notification of data subjects, the Oxford team identified the following reform approaches:

> *The International Principles:* The group would provide individuals with notification of decisions authorizing surveillance with enough time and detail to allow them to appeal, unless notification would seriously jeopardize the purpose of the surveillance.[87]
>
> *The LIBE report:* The report advocated for respect for the principle of user notification.[88]
>
> *The principles of the technology companies*: The technology companies do not discuss this issue.[89]

---

[84] 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.

[85] Brown et al., *supra* note 1, at 10.

[86] 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*, (Apr. 7, 2015), http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e [hereinafter "VENICE COMMISSION REPORT"], at 19, n.38.

[87] *International Principles*, *supra* note 3, at "User Notification"; *see* Brown et al., *supra* note 1, at 22.

[88] *LIBE Report*, *supra* note 4 at para. 22; *see* Brown et al., *supra* note 1, at 22.

[89] The category is not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 22.

The Review Group: The Review Group recommended limits on nondisclosure orders, with service providers being able to provide notice once the order expires.[90] More generally, a theme of this testimony is the importance of creating effective systemic safeguards against excessive surveillance,[91] while being cautious about providing individual notice or individual remedies if they can be used as a vector of attack by hostile actors to national security secrets.[92]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[43] *Review Group Recommendation 8:* "We recommend that:

1. legislation should be enacted providing that, in the use of National Security Letters, section 215 orders, pen register and trap-and-trace orders, 702 orders, and similar orders directing individuals, businesses, or other institutions to turn over information to the government, non-disclosure orders may be issued only upon a judicial finding that there are reasonable grounds to believe that disclosure would significantly threaten the national security, interfere with an ongoing investigation, endanger the life or physical safety of any person, impair diplomatic relations, or put at risk some other similarly weighty government or foreign intelligence interest;
2. nondisclosure orders should remain in effect for no longer than 180 days without judicial re-approval; and
3. nondisclosure orders should never be issued in a manner that prevents the recipient of the order from seeking legal counsel in order to challenge the order's legality."[93]

[44] *Reforms since 2013.* In January 2014, President Obama announced that indefinite secrecy would change for National Security Letters (NSLs). He directed the US Attorney General to change NSL rules so that secrecy about NSLs "will not be indefinite," and "will terminate within a fixed time unless the government demonstrates a real need."[94] As of 2015, the FBI presumptively terminates NSL secrecy for an individual order when an investigation closes, or no more than three years after the opening of a full investigation.[95] Exceptions are permitted only if a senior official determines that national security requires NSL secrecy to be extended in the particular case, and explains the basis in writing.[96]

---

[90] *Id.* at Recommendation 8.
[91] *See generally* Chapter 3.
[92] *See generally* Chapter 8.
[93] *Id.*
[94] *Remarks by the President on Review of Signals Intelligence*, WHITE HOUSE, OFFICE OF PRESS SEC'Y (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [hereinafter *Remarks by the President*].
[95] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform: 2015 Anniversary Report*, IC ON THE RECORD, https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[96] *Id.*

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[45] *Review by Agency for Fundamental Rights:* Eight Member States do not provide a notice obligation or the right to access data collected for foreign surveillance purposes.[97] In Member States that provide a right to access and an obligation for the agency to inform the individual, these rights "tend to be restricted on the ground that the information would threaten the objectives of the intelligence services or national security."[98] In Bulgaria, the rights of notification and access only apply to unlawful surveillance.[99] In Germany, the individual must establish a special interest to be able to exercise the right to access.[100] In Sweden, the data subject has a right to be informed, within a month of the collection, if the search terms directly relate to him/her. As of the date of the Agency for Fundamental Rights Report, no individuals had been informed – due to secrecy reasons.[101]

[46] The Agency for Fundamental Rights Report explained that three Member States have established timeframes that must be exhausted before notice applies and access rights can be exercised.[102] For example, in the Netherlands, individuals are notified five years after the surveillance, such as intercepting telecommunications, has taken place. This five-year deadline for notification can be further postponed if it will affect foreign intelligence information or relations with an ally.[103] The Hague District Court has held that there is not absolute duty of notification, and that, in cases involving surveillance, the secrecy of that surveillance prevails.[104]

[47] Ten Member States have a mechanism to involve the oversight body or court to determine whether the invoked grounds for restricting the rights are reasonable.[105] For example, in Austria, the right to access is restricted if that access could threaten the security of the state. The individual

---

[97] These countries are: the Czech Republic, Ireland, Latvia, Lithuania, Poland, Slovakia, Spain, and the UK. AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 62.
[98] *Id.* at 63.
[99] *Id.*; Закон за специалните разузнавателни средства [Bulgaria Special Intelligence Means Act], Oct. 21, 1997, Нов - ДВ, бр. 109 от 2008 г., изм. - ДВ, бр. 70 от 2013 г., в сила от 09.08.2013 г. [as amended by SG. 109 of 2008, SG. 70 of 2013, effective Aug. 9, 2013] (Bulg.).
[100] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 63; Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG) [German Federal Act on the Protection of the Constitution] Dec. 20, 1990, das zuletzt durch Artikel des Gesetzes vom 26. Juli 2016 [last amended by Article 1 of the Law of July 26, 2016 (I, at 1818)]; Gesetz über den Bundesnachrichtendienst [BNDG] [German Act on the Federal Intelligence Service], Dec. 21, 1990, das zuletzt durch Artikel des Gesetzes vom 26. Juli 2016 (BGBI. I.S.1818) [last amended by Art.2 of the Law of July 26, 2016 (I, at 1818)] at § 7.
[101] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 63; *see also* Wet op de inlichtingen - en veiligheidsdiensten 2002 7 februari 2002 [Intelligence and Security Act 2002, Feb. 7, 2002] (Neth.), at 6.
[102] These countries are Belgium, Croatia, and the Netherlands. AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 63.
[103] *Id.*, at 63-64; *see also* Wet op de inlichtingen - en veiligheidsdiensten 2002 7 februari 2002 [Intelligence and Security Act 2002, Feb. 7, 2002] (Neth.) at Art. 34, 35(7), 47, 53 (Neth.).
[104] Rechtbank Den Haag [Court of the Hague] 23 juli 2014, ECLI:NL:RBDHA: 2014: 8966 (C/09/455237/HA ZA 13-1325, *Dutch Association Criminal Lawyers / Netherlands*) (Neth.), (in Dutch) http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2014:8966.
[105] The countries are: Austria, Belgium, Cyprus, Denmark, France, Germany, Greece, Italy, Luxembourg, and the Netherlands. AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 64-65.

may turn to the Data Protection Authority (DPA) to request a check of the agency's reply, but this process does not confirm or deny that surveillance is occurring.[106]

8. Data Minimization

[48] In the category of data minimization, the Oxford team identified the following reform approaches:

> *The International Principles:* The group called for confining the data accessed to only that which is reasonably relevant and for promptly destroying any excess information collected.[107]
>
> *The LIBE report:* The report does not address the issue.[108]
>
> *The principles of the technology companies:* The technology companies do not address the issue.[109]
>
> *The Review Group:* We recommended extending provisions on data minimization for US citizens under Section 215 of the USA PATRIOT Act to National Security Letters.[110]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[49] *Review Group Recommendation 3:* "We recommend that all statutes authorizing the use of National Security Letters should be amended to require the use of the same oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders."[111]

[50] *Reforms since 2013:* As one mechanism to minimize collection of data, the USA FREEDOM Act prohibited bulk collection via National Security Letters (phone, financial, and credit history records).[112] Furthermore, Presidential Policy Directive 28 (PPD-28) requires US intelligence agencies to apply the same minimization protections to non-US persons that they apply to US persons. Data about non-US persons may only be retained when "retention of comparable information concerning persons would be permitted."[113] Similarly, data about non-US persons cannot be disseminated unless the same could be done with comparable data about US persons.[114]

---

[106] *Id.* at 64; *see* Bundesgesetz über den Schutz personenbezogener Daten [Federal law on the Protection of Personal Data] (Datenschutzgesetz 2000 (DGS2000)) [(Data Protection Act 2000 (DGS2000), as amended)] Bundesgesetzblatt [BGBl] No. 165/1999, as amended, at §§ 26(2), 30(3) (Austria).
[107] *International Principles*, *supra* note 3, at "Proportionality" and "Competent judicial authority"; *see* Brown et al., *supra* note 1, at 22-23.
[108] *LIBE Report*, *supra* note 4, at para. 106; *see* Brown et al., *supra* note 1, at 22.
[109] The category was not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 22.
[110] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 3; *see* Brown et al., *supra* note 1, at 22-23.
[111] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 3.
[112] USA FREEDOM Act, Sec. 501.
[113] *See* PPD-28, *supra* note 29, § 4(a)(i).
[114] *See id.*

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[51] *Review by Oxford team:* No European country "explicitly provides for minimization procedures or remedies for non-citizens."[115] Some European countries have safeguards aimed at minimizing the amount of data held on their own citizens. The Oxford team cited the Netherlands for having a statutory provision that requires the deletion of any data that has been "wrongly collected."[116] Generally, however, the Oxford team found that the laws in European Member States lack detail regarding the purpose, scale, nature, and oversight mechanisms for foreign intelligence surveillance.[117]

[52] The laws of the EU Member States do not explicitly rule out the bulk collection of foreign intelligence. Contrary to a prohibition on bulk collection, it is common for EU Member States' laws to compel telecommunication providers to cooperate with the country's intelligence agencies to allow the agencies access to foreign communications. After the communications are collected, the agencies filter the data based on selectors, which are keywords or personal information. In certain instances, these selectors need to be approved in advance by the executive branch, normally at a ministerial level; they may be subject to periodic review by the government or, in limited instances, there may be oversight by an independent body.[118]

9. Onward Transmission/Purpose Limitation

[53] In the category of onward transmission/purpose limitation, the Oxford team analyzed the following reform approaches:

> *The International Principles:* The groups urged that surveillance should only be accessed by the specified authority and used only for the purpose for which the authorization was given.[119]
>
> *The LIBE report*: The report did not address this issue.[120]
>
> *The principles of the technology companies:* The technology companies did not address this issue.[121]
>
> *The Review Group:* We advocated for no dissemination of information about non-US persons unless the information is relevant to protecting the national security of the US or its allies.[122]

---

[115] Brown et al., *supra* note 1, at 10.
[116] *Id*.
[117] *Id.*
[118] *Id*.
[119] *International Principles*, *supra* note 3, at "Proportionality" and "Competent judicial authority"; *see* Brown et al., *supra* note 1, at 23.
[120] The category is not addressed in the *LIBE Report*; *see* Brown et al., *supra* note 1, at 23.
[121] The category is not addressed in the *Company Principles*; *see* Brown et al., *supra* note 1, at 23.
[122] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 13(4); *see* Brown et al., *supra* note 1, at 23.

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[54] *Review Group Recommendation 13(4):* "We recommend that, in implementing section 702, and any other authority that authorizes the surveillance of non-United States persons who are outside the United States, in addition to the safeguards and oversight mechanisms already in place, the US Government should reaffirm that such surveillance . . . must not disseminate information about non-United States persons if the information is not relevant to protecting the national security of the United States or our allies."

[55] *Reforms since 2013:* The agency procedures put in place pursuant to Section 4 of PPD-28 have created new limits that address this concern.[123] The new retention requirements and dissemination limitations are consistent across agencies and similar to those for US persons.[124] 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.[125] For dissemination, there is an important provision applying to non-US persons collected outside of the US: "personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted."[126]

[56] 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."[127]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[57] *Review by Oxford team:* In EU Member States, the collection of electronic communications from outside the borders of the country is authorized for a variety of purposes. EU Member States have given themselves greater flexibility to do surveillance outside of their borders than within.[128]

10. Transparency

[58] In the category of transparency, the Oxford team identified the following reform approaches:

---

[123] 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. *See* PPD-28, *supra* note 29, at § 4.
[124] The agency procedures create new limits on dissemination of information about non-US persons, and require training in these requirements. *Id.*
[125] There are exceptions to the five-year limit, but they can only apply after the Director of National Intelligence considers the views of Office of the Director of National Intelligence Civil Liberties Protection officer and agency privacy and civil liberties officials. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Strengthening Privacy and Civil Liberties Protections 2015 Anniversary Report*, IC ON THE RECORD, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[126] PPD-28, *supra* note 29, § 4(a)(i).
[127] *Id.*
[128] Brown et al, *supra* note 1, at 10.

The International Principles: The group supported requiring governments to publish periodic reports about foreign intelligence surveillance.[129]

The LIBE report: The report only spoke of transparency in general terms.[130]

The principles of the technology companies: The technology companies sought the ability to publish the number and nature of government demands for user information, and a requirement for governments to publicly disclose this information.[131]

The Review Group: We recommended increased transparency, both through government reporting and by permitting private sector recipients of government requests to provide more detail.[132]

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[59] *Review Group Recommendation 9:* "We recommend that legislation should be enacted providing that, even when nondisclosure orders are appropriate, recipients of National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders issued in programs whose existence is unclassified may publicly disclose on a periodic basis general information about the number of such orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security."[133]

[60] *Review Group Recommendation 10:* "We recommend that, building on current law, the government should publicly disclose on a regular basis general data about National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders in programs whose existence is unclassified, unless the government makes a compelling demonstration that such disclosures would endanger the national security."[134]

[61] *Reforms since 2013:* In January, 2014 the US Department of Justice changed its reporting policies in response to litigation by five technology companies – Google, Microsoft, Yahoo, LinkedIn, and Facebook – to permit companies to report broad ranges of the numbers of orders they receive for collection of user information.[135] The USA FREEDOM Act codified and expanded

[129] *International Principles*, *supra* note 3 at "Public oversight"; *see* Brown et al., *supra* note 1, at 23.
[130] *LIBE Report*, *supra* note 4 at para. 62; *see* Brown et al., *supra* note 1, at 23.
[131] *Company Principles*, *supra* note 5, para. 2; *see* Brown et al., *supra* note 1, at 23.
[132] REVIEW GROUP REPORT, *supra* note 6, at Recommendations 9, 10; *see* Brown et al., *supra* note 1, at 23.
[133] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 9.
[134] *Id.* at Recommendation 10.
[135] *See* Letter of January 27, 2014 from James M. Cole, Deputy Attorney General, US 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.).

this agreement. 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.[136] Companies can report ranges of the number of (1) National Security Letters, (2) FISA orders or directives, and (3) non-content requests – along with the "number of customer selectors" targeted under each such request.[137] They may report ranges of the "total number of all national security process received," as well as the number of customers affected by such requests.[138]

[62] The USA FREEDOM Act codified expansion in the annual reporting by the US government about its national security investigations.[139] 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 *amicus curiae* as well as any findings that an appointment was not appropriate.[140]

[63] Administratively, the Office of the Director of National Intelligence's January 2015 report on Signals Intelligence Reform detailed eight categories of greater transparency that it had undertaken to that point.[141] Compared to the secrecy that historically had applied to signals intelligence, the shift toward greater transparency is remarkable, such as:

- The declassification of numerous FISC decisions;[142]
- A new website devoted to public access to intelligence community information;[143]
- The first "Principles of Intelligence Transparency for the Intelligence Community;[144]
- The first three Intelligence Community Statistical Transparency Reports;[145]

[136] USA FREEDOM Act, Sec. 604 (codified at 50 U.S.C. § 1874(a)).
[137] *See* 50 U.S.C. § 1874(a)(1).
[138] *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).
[139] USA FREEDOM Act § 603.
[140] *Id.* §§ 601-602.
[141] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform, 2015 Anniversary Report – Enhancing Transparency*, IC ON THE RECORD (2015), https://icontherecord.tumblr.com/ppd-28/2015/enhancing-transparency.
[142] For detailed discussion of the rulings in these opinions, see Chapter 5.
[143] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Declassified: Release of FISC Question of Law and FISCR Opinion*, IC ON THE RECORD (Aug. 22, 2016), http://icontherecord.tumblr.com.
[144] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Principles of Intelligence Transparency for the Intelligence Community*, http://www.dni.gov/files/documents/ppd-28/FINAL%20Transparency_poster%20v1.pdf; 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.
[145] 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.

- Unclassified reports on NSA's implementation of Section 702[146] and its "Civil Liberties and Privacy Protections for Targeted SIGINT Activities;[147]
- 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;[148] and
- The Office of Director of National Intelligence now has a Civil Liberties Protection Officer.[149]

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[64] Transparency about EU practices comes notably from public reviews in recent years, including:

1. *Review commissioned by the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs:* The 2013 briefing paper of the Center for European Policy Studies (CEPS) is approximately 75 pages, focusing on large-scale surveillance programs in the US and the EU.[150]

2. *Review by the Council of Europe's Commissioner of Human Rights*: The 2015 report is approximately 75 pages and details oversight of intelligence services.[151]

3. *Review by the European Union Agency for Fundamental Rights*: The 2015 report, which is approximately 100 pages, analyzes intelligence services and surveillance laws, oversight of intelligence services, and remedies.[152]

4. *Review by Venice Commission:* The 2015 report is approximately 40 pages and discusses democratic control, jurisdiction, accountability, and controls.[153]

---

[146] NATIONAL SECURITY AGENCY, *Civil Liberties and Privacy Home* (May 3, 2016), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf.
[147] 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.
[147] NATIONAL SECURITY AGENCY, *Civil Liberties and Privacy Home* (May 3, 2016), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf.
[148] 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.
[149] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, OFFICE OF CIVIL LIBERTIES, PRIVACY AND INTELLIGENCE, *Who We Are*, https://www.dni.gov/index.php/about/organization/civil-liberties-privacy-office-who-we-are.
[150] Bigo, et al., *supra* note 32, at 1-76.
[151] COUNCIL OF EUROPE COMMISSIONER OF HUMAN RIGHTS, ISSUE PAPER: DEMOCRATIC AND EFFECTIVE OVERSIGHT OF NATIONAL SECURITY SERVICES 1-74 (2015), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770.
[152] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 1-95.
[153] VENICE COMMISSION REPORT, *supra* note 87, at 1-39.

5. *Review by Professor Federico Fabrinni:* Approximately 30 pages in length, the 2015 article examines the privacy implications of the *Digital Rights Ireland* case.[154]

6. *Review by Dr. Christina Casagran*: This recently published book is approximately 240 pages. It highlights data protection relating to surveillance for law enforcement and foreign intelligence purposes.[155]

7. *Review by Oxford team:* The 2016 paper is approximately 40 pages and concentrates on existing foreign intelligence gathering standards, state obligations under international law, and proposals for surveillance reform.[156]

11. Oversight

[65] In the category of oversight, the Oxford team identified the following reform approaches:

The International Principles: The group proposed independent mechanisms that ensure transparency and accountability and have the authority to access all potentially relevant information about state actions.[157]

The LIBE report: The report urged oversight based on a strong legal framework, ex ante authorization, and ex post verification as well as adequate technical capability and expertise.[158]

The principles of the technology companies: The technology companies advocated for strong checks and balances. [159]

The Review Group: We recommended that the Director of National Intelligence establish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers. To this end, the Director of National Intelligence should prepare an annual report on this issue to the National Security Advisor, to be shared with the Congressional Intelligence committees.[160]

---

[154] Federico Fabrinni, *Human Rights in the Digital Age: The European Court of Justice Ruling in Digital Rights Ireland and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUM. RTS J. 65 (2015), http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf.
[155] Cristina Blasi Casagran, *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, (New York: Routledge 2017), at 1-244.
[156] Brown et al., *supra* note 1, at 1-41.
[157] *International Principles*, *supra* note 3 at "Public oversight"; *see* Brown et al., *supra* note 1, at 23-24.
[158] *LIBE Report*, *supra* note 4, at ¶¶ 74-79; *see* Brown et al., *supra* note 1, at 23-24.
[159] *Company Principles*, *supra* note 5, ¶ 2; *see* Brown et al., *supra* note 1, at 23.
[160] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 18; *see* Brown et al., *supra* note 1, at 22-23.

a. The Approach Recommended by the Review Group and Subsequent US Reforms

[66] *Review Group Recommendation 18:* "We recommend that the Director of National Intelligence should establish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers. To this end, the Director of National Intelligence should prepare an annual report on this issue to the National Security Advisor, to be shared with the Congressional intelligence committees."[161]

[67] *Reforms since 2013:* In a close match with Review Group Recommendation 18, President Obama in 2014 announced that he was creating a process for senior policymakers to monitor the collection and dissemination activities of the Intelligence Community.[162]

[68] Since the Snowden revelations, the US has performed independent oversight through the Review Group and the Privacy and Civil Liberties Oversight Board (PCLOB).[163] Among other findings of the Review Group, we found strong compliance with existing requirements and no improper use of surveillance against political opponents.[164] We saw no instances of abuse of government power for inappropriate purposes, such as suppression of minorities, influencing of elections, or punishment of political opponents.

[69] Since 2013, the PCLOB has released detailed reports on Section 215 and 702 programs, making numerous recommendations.[165] Its central recommendations on telephone metadata program were enacted in the USA FREEDOM Act.[166] It made ten recommendations concerning Section 702, and virtually all have been accepted and either implemented or are in the process of being implemented.[167] In addition to the independent review by the Review Group and the PCLOB, Chapter 3 discusses the entire system of oversight that exists for foreign intelligence investigations, including the Foreign Intelligence Surveillance Court discussed in more detail in Chapter 5.

---

[161] REVIEW GROUP REPORT, *supra* note 6, at Recommendation 18.
[162] *See Remarks by the President*, *supra* note 94.
[163] 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.
[164] REVIEW GROUP REPORT, *supra* note 6, at 78, 182.
[165] *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.
[166] This focused on Section 215 of FISA.
[167] For a list of the PCLOB's ten recommendations and the government's implementation actions in response, *see* Chapter 3, Section IV(C).

b. Review of European Practices by EU Commentators since the Snowden Disclosures

[70] *Review by Oxford team:* The Oxford team explained that the quality of oversight depends on the resources available, the technical competence of the reviewers, and the avoidance of regulatory capture.[168] In its review, the Oxford team cited to the LIBE report, calling for oversight bodies to conduct on-site visits of intelligence agencies, interview senior officials, and ensure independence of inspectors. Both the Review Group and the PCLOB have had these characteristics.

[71] *Review by the European Union Agency for Fundamental Rights:* The Agency for Fundamental Rights Report noted that the general consensus is that oversight of foreign surveillance should combine executive control; parliamentary control; judicial review; and expert bodies:[169]

> Effective oversight does not necessarily require all four types of oversight mechanisms. Such oversight can be accomplished as long as the bodies in place complement each other and as a whole constitute a strong system capable of assessing whether the intelligence services' mandate is carried out properly.[170]

[72] The Agency for Fundamental Rights determined 24 EU Member States have parliamentary oversight, and 15 Member States have set up at least one expert body dedicated to the oversight of intelligence agencies.[171] The report analyzed the authority of Data Protection Authorities in EU Member States and determined that 12 of 28 have Data Protection Authorities with no power over national intelligence agencies, and another nine have limited powers related to intelligence.[172] Seven Member States have oversight systems that combine the executive, parliament, judiciary, and expert bodies. These seven Member States, however, do not include any of the Member States that have legal frameworks allowing signals intelligence collection.[173]

[73] With regard to signals intelligence, the report identified five Member States – France, Germany, the Netherlands, Sweden, and the UK – that engage in signals intelligence and have detailed legislation in place regarding this activity.[174] France has executive oversight, with the Prime Minister authorizing selectors and opinions offered by an oversight board.[175] The Netherlands collects non-cable bound communications (satellite and radio transmissions) without authorization outside of the agency, but must seek executive oversight for access using

---

[168] Brown et al., *supra* note 1, at 31.
[169] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 29; VENICE COMMISSION REPORT, *supra* note 87.
[170] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 57.
[171] *Id.* at 57-58.
[172] *Id*. at 49.
[173] *Id*. at 57.
[174] *Id*. at 20.
[175] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 56; *see* CODE DE LA SÉCURITÉ INTÉRIEURE [INTERIOR SECURITY CODE] Art L. 851-3 (Fr.), *La localisation, la sonorisation de certains lieux et véhicules, la captation d'images et de données informatiques*, http://www.assemblee-nationale.fr/14/projets/pl2669.asp.

keywords.[176] The UK requires warrants authorized by the Secretary of State.[177] The UK has an Investigatory Powers Tribunal to deal with individual complaints concerning surveillance, but its authority is limited to "assessing whether legislation has been complied with and authorities have acted 'reasonably.'"[178] Germany has oversight from both the Parliamentary Control Panel (telecommunications) and the G-10 Commission (selectors to filter the data).[179] Sweden has oversight by an expert body.[180]

[74] One of the Agency for Fundamental Rights' key findings was: "Access to information and documents by oversight bodies is essential. While information gathered by intelligence bodies is sensitive, and safeguards must guarantee that it will be dealt with accordingly, oversight bodies cannot carry out their tasks without first having access to all relevant information. The opposite, however, seems to be the norm [in the EU]."[181]

[75] *Review commissioned by the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs:* The briefing paper of the Center for European Policy Studies (CEPS) found that several Member States have oversight bodies that are faced with constraints that hamper their ability to apply sufficient scrutiny to intelligence agencies' surveillance practices. In Sweden, the two main oversight institutions, the intelligence court (UNDOM) and the Inspection for Defense Intelligence Operations (SIUN), were "deemed to be insufficiently independent." In France, the main oversight body, the CNCIS, was "found to be substantially constrained in its reach due to its limited administrative capacity."[182]

II. Conclusion

[76] The Oxford team found that the US legal system of foreign intelligence law contains "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."[183]

---

[176] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 55; *see* Wet op de inlichtingen - en veiligheidsdiensten 2002 7 februari 2002 [Intelligence and Security Act 2002, Feb. 7, 2002] at Art. 26 (Neth.).
[177] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 55; s*ee* INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK, 2015, HC 1075, at 37-38 (UK), *visit* http://isc.independent.gov.uk/committee-reports/special-reports *and click on* "Privacy and Security: a modern and transparent legal framework."
[178] AGENCY FOR FUNDAMENTAL RIGHTS REPORT, *supra* note 61, at 68.
[179] *Id.* at 55.
[180] *Id.* at 54.
[181] *Id.* at 57. For example, in Poland, the prime minister appoints and dismisses the heads of the Polish intelligence services. She/he is in charge of approving their intelligence objectives and has the most far-reaching competences in terms of oversight of the intelligence services within the country. However, the Supreme Audit Office found that his/her oversight lacks efficacy, since he/she does not have access to the internal procedures of the intelligence services. The information given by the services both as to the content and the means by which intelligence is collected cannot therefore be verified. *Id.* at 32.
[182] Bigo et al., *supra* note 32, at 26.
[183] Brown et al., *supra* note 1, at 3. *See* Chapter 3 for a detailed discussion of the US system of foreign intelligence law.

[77] To the extent that the specifics of the EU Member States' legal frameworks for foreign intelligence surveillance are publicly available,[184] the Oxford team determined that "they generally compare unfavorably with the situation in the US after the adoption of [Presidential Privacy Directive 28]."[185]

[78] As the analysis in the article by the Oxford team charts, the Review Group made recommendations in most or all of the 11 categories identified by the Oxford team, and the US government has undertaken reforms in most or all of the categories since the release of the Review Group's recommendations.

[79] In conclusion, this independent framework for analysis provides a systematic and relatively objective tool to support my view that the safeguards in the US system of foreign intelligence law compare favorably to the regimes in other nations.

[184] Despite the limitations on the publicly available laws and procedures regulating foreign intelligence surveillance, the Oxford team found that the acts of the EU Member States share similar structures and that many European countries have made similar policy choices in respect to regulating foreign intelligence surveillance.

[185] Brown et al., *supra* note 1, at 10. After analyzing the laws of EU Member States, the Oxford team pointed out that European governments that want to further limit the NSA's activities concerning EU citizens first "need to get their own houses in order by developing, publicizing, and adopting publicly available standards that govern foreign intelligence collection." *Id.* at 10-11.

CHAPTER 7:

INDIVIDUAL REMEDIES IN US PRIVACY LAW

[1] The US legal system provides numerous ways for an individual to remedy violations of privacy. I have sometimes encountered the view in the EU that the US lacks remedies for privacy violations generally. That is not correct. I am the lead author of the textbook for the International Association of Privacy Professionals (IAPP) for the certification exam on US private-sector privacy law.[1] We published the second edition in 2012, and we are now preparing publication of the third edition. With only an introductory overview of US privacy laws that apply to the private sector, including enforcement mechanisms, the second edition took nearly 200 pages and eleven chapters,[2] and the third edition will be longer. That book documents many aspects of US privacy law that do not fit in this Chapter.

[2] The large quantity of US privacy law sometimes leads to a different critique from the EU: that US remedies are "fragmented" and may for that reason not be adequate under EU standards. This Chapter aims to help explain how the different pieces of US law fit together. The complexity of US law in part comes from the fact that more than one source of enforcement can exist for any given privacy issue. This division of authority can be beneficial for privacy protection, as it allows subject matter experts to enforce in areas they understand best, allows multiple agencies to police categories of activity on behalf of data subjects, and also allows private rights of action for individuals.

[3] Scholars have noted the breadth of remedies available to individuals in the US and their impact on the privacy-protecting behaviors of US companies. Professors Kenneth A. Bamberger and Deirdre K. Mulligan's book *Privacy on the Ground* studied corporate behavior in five countries, and found that US companies often have stronger privacy management practices.[3] Professor Danielle Citron's award-winning article *The Privacy Policymaking of State Attorneys General* similarly shows how the work of state Attorneys General (AGs) in the US serve as "laboratories of privacy enforcement."[4] Citron explains how state AGs can take a more nimble approach to privacy enforcement than a single federal enforcement agency, allowing them to respond faster to concerns raised in the press or by the public.[5] The multiple US privacy laws have a strong influence, in my view, on the practices of US companies, who face enforcement actions if they do not have effective compliance with the law and their stated privacy policies.[6]

---

[1] PETER SWIRE & KENESA AHMAD, U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS (2012) [hereinafter SWIRE & AHMAD, U.S. PRIVATE SECTOR PRIVACY]. The same year, we published a book providing an introduction to privacy globally. PETER SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS, AND PRACTICES (2012).

[2] *Id.*

[3] *See generally* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015).

[4] Danielle Keats Citron, *Privacy Policymaking of State Attorneys General*, NOTRE DAME L. REV. (forthcoming) (manuscript at 1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.

[5] *Id.* (manuscript at 4).

[6] *See, e.g.*, GOOGLE, *Privacy Policy*, https://www.google.com/policies/privacy/ (last updated Aug. 29, 2016) ("We will share personal information with companies, organizations, or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to: meet any applicable law, regulation, legal process or enforceable governmental request"); MICROSOFT, *Privacy Statement*, https://privacy.microsoft.com/en-US/privacystatement (last updated Sep. 2016) ("We share your personal data . . . when required by law or to respond to legal process"); TWITTER, *Privacy Policy*, https://twitter.com/privacy?lang=en (last updated Sep. 30, 2016) ("[W]e may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request.").

[4] This Chapter outlines the steps an aggrieved individual, whether in the US or in the EU, may take in response to concerns regarding US privacy violations. Section I examines individual judicial remedies against the US government. These remedies feature two recently-finalized agreements with the EU, the Privacy Shield and the Umbrella Agreement, as well as the Judicial Redress Act whose passage the EU strongly supported. It next examines the civil and criminal remedies that exist where individuals, including government employees, violate the wiretap and other surveillance rules under laws such as the Stored Communications Act, the Wiretap Act, and the Foreign Intelligence Surveillance Act.

[5] Section II examines non-judicial remedies available to individuals concerned about US government actions. I highlight three paths — the Privacy and Civil Liberties Oversight Board, Congressional committees, and recourse to the US free press and privacy-protective non-government organizations. Both US-persons and EU persons can benefit from the ability to make complaints in these ways, and gain a multiplier effect as the agency, Congressional committee, or privacy advocacy organization takes up the cause.

[6] Section III examines individual remedies against US companies, such as service providers of webmail and social networks, should they improperly disclose information to the US government about customers. It then examines privacy enforcement by five federal administrative agencies, including the Federal Trade Commission (FTC) and Federal Communications Commission (FCC). These administrative agencies do not themselves bring actions against intelligence agencies. They can be important, however, because they can bring actions against companies that fail to comply with applicable law or company privacy policies, such as when the companies improperly provide electronic communications to the government.

[7] Section IV introduces privacy enforcement under state law and private rights of action. Each state has an Attorney General tasked with protecting consumers. As documented by Professor Citron, these AGs have emerged as important privacy enforcers. It then examines the numerous private rights of action that exist under US law, using the state of California as one example. These lawsuits on behalf of individuals are a well-known feature of US law. During negotiation of the Safe Harbor in 1999-2000, I heard US Ambassador David Aaron, the lead US negotiator, say more than once to EU negotiators: "We'll take your privacy laws if you'll take our plaintiffs' lawyers." The prevalence of plaintiffs' lawyers and private rights of action in the US means that defendants (including companies and often government agencies) have increased incentive to comply strictly with applicable law.

[8] Section V examines issues of who has standing to sue in the wake of the 2013 US Supreme Court case of *Clapper v. Amnesty International USA*. Section VI offers conclusions.

[9] This chapter contains two Annexes. The first is a chart that lists US privacy remedies and safeguards, specifically noting those that are available to EU persons, and not only to US persons. The second is a chart detailing major privacy settlements in the US from 2006 through 2016. This chart illustrates the substantial magnitude of class action and agency enforcement, as discussed in Section IV of this chapter.

[10] Before turning to the individual remedies, I briefly discuss the intersection of individual remedies with the systemic safeguards discussed in Chapters 3, 4, and 5. Systemic safeguards have a notable advantage in creating limits on intelligence agencies – oversight agencies can gain access to classified information, and methodically examine otherwise-secret agency practices. In the US, oversight actors with access to classified information include the Foreign Intelligence Surveillance Court, the PCLOB, agency Inspectors General, the Senate and House Intelligence Committees, and other bodies such as the Review Group on which I served. With access to the classified information, these actors can detect privacy problems and take action to correct them. By contrast, as discussed in Chapter 8, there is a caveat to the desirability of individual remedies – there are reasons to be cautious about disclosing national security secrets in open court or to an individual who may be probing the intelligence system rather than honestly seeking to correct a privacy violation.

[11] As a related point, systemic safeguards can more specifically bolster or parallel individual remedies. For example, the US system of foreign intelligence law places surveillance authorization in the hands of a court – the Foreign Intelligence Surveillance Court engages in a specific proceeding, determining whether surveillance satisfies statutes and the Constitution.[7] The rules for Section 702 collection require data acquired as a result of a compliance incident to be purged, as would occur through a successful individual deletion request.[8] Transparency mechanisms, such as governmental or corporate transparency reports, provide information about the scope of government surveillance programs akin to what individual information requests may seek.[9] The US system of foreign intelligence safeguards thus reinforces the individual remedies discussed in this Chapter in the interest of protecting the rights those remedies seek to vindicate.

I. Individual Judicial Remedies against the US Government

[12] In the US, persons who suffer a privacy harm can seek remedies in both civil and criminal cases. This section focuses on actions that an individual can bring in state or federal courts in the US. Section II below addresses multiple administrative/regulatory processes that can be undertaken to respond to assertions of privacy related issues. This subsection first discusses civil actions an individual can take, focusing on civil remedies available against the US government,[10] and then provides a parallel analysis for remedies through criminal proceedings. It also responds to specific critiques of US privacy remedies by the Irish Data Protection Commissioner.

---

[7] *See* Chapter 3, Section III(A). An interlocking system of audits and reporting provides the Foreign Intelligence Surveillance Court (FISC) with notices of compliance incidents, and the FISC has responded strongly to compliance incidents. *See* Chapter 5, Section II(A).

[8] In Section 702 collection, "[i]f the data was acquired as a result of a compliance incident," such as a "typographical error" or "an overproduction by the provider," the "acquired communications must be purged." PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 49 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.

[9] For an extensive discussion on transparency safeguards in US surveillance law, *see* Chapter 3 ("Systemic Safeguards in the US System of Foreign Intelligence Surveillance Law").

[10] Under US law, litigation can be conducted against the government itself as well as actors acting "under the color of governmental authority," such as contractors hired to conduct surveillance or otherwise act on the government's behalf. *See, e.g.*, 42 U.S.C. § 1983 ("Every person who, under color of any statute, ordinance, regulation, custom, or usage . . . shall be liable").

A. US Civil Judicial Remedies

[13] Civil suits allow qualifying individuals, including EU persons, to sue the US government for violations of law that can result in monetary damages and injunction of ongoing illegal actions. Unlike criminal violations of law, which must be prosecuted by an agent of the government, any qualifying individual can bring a civil suit as long as he or she meets the thresholds required for the alleged wrongful act.[11] Likewise, certain administrative agencies can also seek civil penalties for violations of US law and regulations. While the US, like most sovereigns, generally reserves immunity from suit, the US government has waived that sovereign immunity by statute in circumstances that are relevant to redress of individual privacy concerns.[12]

1. Judicial Redress Act, Privacy Shield, and the Umbrella Agreement

[14] The Judicial Redress Act, the EU-US Privacy Shield, and the Data Protection and Privacy Agreement (i.e., the Umbrella Agreement) combine to provide new individual legal remedies for EU persons who believe they have suffered privacy harms, in addition to those specified by the Standard Contractual Clauses (SCCs) themselves.

[15] Under the Judicial Redress Act,[13] the US expressly extended the right to a civil action against a US governmental agency to obtain remedies with respect to the willful or intentional disclosure of covered records in violation of the Privacy Act to qualified individuals.[14] The Judicial Redress Act also extends the right to a civil action against a designated US governmental agency or component when that agency or component declines to amend the record in response to a qualifying individual's request.[15] A qualifying individual is one who has been subject to improper response to a request from a US agency.[16] The Act allows US and qualifying non-US persons to sue a US federal agency for the improper handling of their data; to obtain injunctions

---

[11] *See, e.g.*, 18 U.S.C. § 2707(a) ("[A]ny provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter . . . may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation"); 18 U.S.C. §2520(a) ("[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity").

[12] *See, e.g.*, 5 U.S.C. § 552a(g)(1) (permitting civil action against a US federal agency which violates the statute).

[13] 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 (codified at 5 U.S.C. § 552a).

[14] *Id.* at § 2(a) ("With respect to covered records, a covered person may bring a civil action against an agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring and obtain with respect to records under: (1) section 552a(g)(1)(D) of title 5, United States Code, but only with respect to disclosures intentionally or willfully made in violation of section 552a(b) of such title; and (2) subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, but such an action may only be brought against a designated Federal agency or component.").

[15] *Id.* (citing the availability of civil action under subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, which reads: "Whenever any agency (A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection; (B) refuses to comply with an individual request under subsection (d)(1) of this section . . . the individual may bring a civil action against [a designated Federal agency or component].").

[16] *Id.*

or monetary damages; and to review, copy, and request amendments to their data.[17] In contrast to some of the statutes discussed below, these suits are brought against the agency itself rather than against an individual actor within the agency.[18]

[16] Prior to the passage of the Judicial Redress Act in 2016, an action under the Privacy Act could be brought only by "US persons," who are US citizens or non-citizen permanent residents. Under the Judicial Redress Act, non-US persons may bring a cause of action listed under the Privacy Act if the US Attorney General, in consultation with the Secretaries of State, Treasury, and Homeland Security, designates that the non-US person's country of citizenship "has entered into an agreement with the United States that provides for appropriate privacy protections" and that the country permits the transfer of personal data for commercial purposes to the US.[19] Although EU member states have not to date been individually identified as required under the Judicial Redress Act, my understanding is that the EU and US plan to finalize that process.

[17] Under the EU/US Privacy Shield, the US has created new remedies against the US government available to EU persons. For complaints concerning US government actions, EU data subjects can lodge a complaint with an Ombudsman within the Department of State.[20] The Ombudsman will respond to individuals who file complaints related to the Privacy Shield and inform them whether or not the laws relevant to their situation have been violated.[21] Importantly, this Ombudsman is independent from US national security services.[22] The Ombudsman can be used to process "requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs) [and] binding corporate rules (BCRs)."[23] Indeed, the US and the EU Commission have made clear that the Ombudsman mechanism "is not Privacy Shield specific" and "covers all complaints relating to all personal data and all types of commercial transfers from the EU to companies in the US."[24] Any

---

[17] *Id.* (citing 5 U.S.C. § 552a); see also 5 U.S.C. §§ 552a(g)(2)(A)-(B) (providing that in any suit under 5 U.S.C. § 552a(g)(1), "the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct" and that "[t]he court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed").

[18] *Id.* ("[S]uch an action may only be brought against a designated Federal agency or component").

[19] Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282, § (d)(1) (2015). https://www.congress.gov/bill/114th-congress/house-bill/1428/text.

[20] European Commission Press Release MEMO/16/434, EU-U.S. Privacy Shield: Frequently Asked Questions (Feb. 29, 2016), http://europa.eu/rapid/press-release_MEMO-16-434_en.htm. Note that, as of today, this mechanism is still being organized and is not yet available. *See* PRIVACY SHIELD FRAMEWORK, *How to Submit a Request Relating to U.S. National Security Access to Data* (Oct. 9, 2016), https://www.privacyshield.gov/article?id=How-to-Submit-a-Request-Relating-to-U-S-National-Security-Access-to-Data.

[21] European Commission Press Release, *supra* note 20.

[22] *Id.*

[23] European Commission, Annexes to the Commission Implementing Decision 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, C(2016) 4176 final at 52 (July 12, 2016) [hereinafter "Annexes"], http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf. Note that the Ombudsman can also review requests submitted in response to data transmitted from the EU to the US under derogations and possible future derogations.

[24] European Commission Directorate General for Justice and Consumers, *European Commission Guide to the EU-U.S. Privacy Shield*, at 19 (2016), http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf.

written commitments from the Ombudsman in response to individual inquiries will also be published in the US Federal Register, offering transparent evidence of review.[25]

[18] Individuals in the EU have multiple methods for redress against companies, rather than the US government, for privacy complaints. First, individuals can invoke, free of charge, an independent alternative dispute resolution (ADR) body to handle any complaints against US Privacy Shield companies.[26] Information on and a link to the ADR must be provided on the company's website, and the ADR must be able to "impose effective remedies and sanctions" in response to valid complaints.[27] Second, individuals can file a complaint with an EU Data Protection Authority (DPA), which have their existing enforcement powers today under national law and will gain additional enforcement powers when the General Data Protection Regulation goes into effect in 2018.[28] The Privacy Shield also allows US companies to opt for using an EU DPA as its independent recourse mechanism, and DPA oversight is mandatory when a company handles personnel data transfers from the EU to the US. Individual complaints to the DPA can result in advice delivered to the company and made public to the extent possible. Third, if the company fails to comply with the DPA's advice within 25 days, the DPA may refer the issue to the Federal Trade Commission (FTC) for enforcement. Under Section 5 of the FTC Act, the Commission can bring an enforcement action for a "deceptive" practice if the company promises to comply with Privacy Shield but fails to do so. Fourth, if the company fails to comply with the DPA's advice within 25 days, the DPA may also refer the matter to the Department of Commerce to determine if the company's non-compliance should result in removal from the Privacy Shield List.[29]

[19] The Umbrella Agreement provides remedies for EU citizens whose data is transferred to US law enforcement authorities. Any individual will be entitled to access their personal information – subject to certain conditions, given the law enforcement context – and request corrections if it is inaccurate.[30] Similarly, individuals are entitled to seek correction or rectification of personal information that they assert is either inaccurate or improperly processed.[31] If the petition for access, correction, or rectification is denied or restricted, the authority must provide an explanation of the basis for its denial "without undue delay."[32] The Agreement provides that, if

---

[25] *Id.* The Federal Register is an official record of US government actions, available at https://www.federalregister.gov.

[26] Annexes, *supra* note 23, at 19; *European Commission Guide to the EU-U.S. Privacy Shield*, *supra* note 24, at 12.

[27] *European Commission Guide to the EU-U.S. Privacy Shield*, *supra* note 24, at 15.

[28] *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 70, 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476055364678&uri=CELEX:32016R0679 (outlining the tasks of the newly established Data Protection Board under the Directive).

[29] *Id.*

[30] *See* European Commission Proposal for a Council Decision on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses at 10-12, COM (2016) 237 final (Apr. 29, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476055815798&uri=CELEX:52016PC0237.

[31] *Id.*

[32] *Id.*

the US authority denies a request, the EU citizen may seek judicial review of that decision.[33] An EU citizen may also petition for judicial review of alleged willful or intentional unlawful disclosure of his or her information, for which the court may award compensatory damages where appropriate.[34] The US passed the Judicial Redress Act in part to fulfill this requirement of the Umbrella Agreement.[35]

[20] Standard Contractual Clauses, when implemented by a US company, also offer individual privacy remedies. Under Commission Decision C(2004)5721, "[e]ach party shall be liable to the other parties for damages it causes by any breach of these clauses" and to "data subjects for damages it causes by any breach of third party rights" under the SCCs.[36] Data subjects are also specifically empowered to enforce the SCCs as a third party beneficiary against the data importer or the data exporter with regards to that individual's personal data.[37] The importer and exporter both agree to allow such suit to be adjudicated in the data exporter's country of establishment.[38]

[21] Where a data subject alleges that the data importer has breached the SCCs, the subject is required to request that the data exporter enforce the data subject's rights against the importer.[39] If the data exporter does not take such action within a reasonable period (typically one month) then the data subject may proceed to enforce his or her rights against the data importer directly.[40] The data subject may also file suit against the data exporter in this case for failure "to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses."[41]

2. Electronic Communications Privacy Act – Stored Communications Act

[22] The Electronic Communications Privacy Act (ECPA) specifically creates an individual right of action for individual data subjects, including EU citizens. The Stored Communications Act (SCA) governs access to stored communications data. It provides individual remedies for data subjects whose stored communications data that has been unlawfully accessed or used by either an individual government actor or US agency as a private third party actor which accesses a network without authorization. The protections for access to an individual's stored data are not limited by citizenship and all remedies available under the Act are likewise available to EU citizens as well as US citizens.[42]

---

[33] *Id.* at 12.
[34] *Id.*
[35] *See* 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.
[36] European Commission Decision C(2004)5217, Set II: Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers), http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_set_ii_c2004-5721.doc.
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] 18 U.S.C. § 2510(6) (defining "person" under the statute without restrictions based on citizenship); *see also Suzlon Energy v. Microsoft*, 671 F.3d 726, 730 (9th Cir. 2011),

[23] Under ECPA, different standards apply for judicial orders for US government access, depending on the type of data requested. The strictest of the applicable standards applies the Fourth Amendment's constitutional rule of probable cause of a crime as determined by an independent judge. That probable cause standard now applies to the stored content of electronic communications, including email.[43] Easier access is permitted to what historically has been called "pen register" and "trap and trace" information, the metadata about the communication. To access this dialing, routing, addressing, and signaling information, the government must certify to the judge that that the information likely to be obtained is relevant to an ongoing criminal investigation.[44] Fourth, basic subscriber information (e.g., account name, information provided during account creation) can be voluntarily disclosed to the government upon request, or can be obtained through other judicial process such as a grand jury subpoena.[45]

[24] For violations of these rules, the data subject may bring a civil suit against the agency and/or the individual, even if the data subject is not a US citizen.[46] Suits against both individual officers and US agencies must demonstrate that the violation of ECPA was "willful."[47] If a suit against an individual officer succeeds, the data subject may receive money damages of at least $1,000 USD, equitable or declaratory relief, reasonable attorney's fees, reimbursement of legal fees, and/or punitive damages.[48] The government employee found to have willfully or intentionally violated ECPA may also be subject to discipline for their actions.[49] Suits against a US agency may result in actual damages or $10,000 USD, whichever is greater, plus litigation costs.[50]

---

http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf ("Thus, the Court remains firm in its initial finding that the ECPA unambiguously applies to foreign citizens.").

[43] The statute itself applies varying standards for access to the content of an email, depending on factors such as whether the email has been opened and how old it is. 18 U.S.C. § 2703. Based on the Fourth Amendment, however, a federal appellate court held in the leading *Warshak* case that individuals have a reasonable expectation of privacy in the contents of an email, and that the relatively strict probable cause standard applies. *United States v. Warshak*, 631 F.3d 266, 274 (6th Cir. 2014), http://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf. The US government has publicly stated that it seeks the content of an email under that probable cause standard. *See ECPA (Part 1): Lawful Access to Stored Content: Hearing before the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, Department of Justice), https://judiciary.house.gov/_files/hearings/printers/113th/113-16_80065.PDF.

[44] 18 U.S.C. §§ 3121-22.

[45] *Id.* §§ 2702-03.

[46] *Id.* § 2510; *see also Suzlon Energy v. Microsoft*, 671 F.3d 726, 730 (9th Cir. 2011), http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf.

[47] 18 U.S.C. § 2520. The civil provision requiring "willful" violation has exceptions for good faith reliance on court orders, grand jury subpoenas, legislative authorizations, statutory authorizations, or a valid request from an investigative or law enforcement officer. 18 U.S.C. § 2520(d). Similarly, there is no "willful" violation where the individual or agency being sued made a good faith determination that the alleged action was valid under ECPA. *Id.*

[48] 18 U.S.C. § 2707(c).

[49] *Id.* § 2707(d).

[50] 18 U.S.C. § 2712(a).

3. ECPA – The Wiretap Act

[25] Like the SCA, the Wiretap Act creates an individual right of action against unlawful government action.[51] The rules for getting a wiretap – a real-time interception of a data subject's communications – are even stricter than the usual probable cause standard. To get a wiretap, in addition to probable cause,[52] the government must meet a number of other standards, including seriousness of the crime[53] and an explanation of why the communications sought could not feasibly be obtained by other means.[54] Authorizations for wiretaps must be for a specific and limited time[55] and must include minimization of non-relevant information to protect the privacy of interceptees.[56] Continued surveillance outside that timeframe without separate judicial authorization is considered unlawful.[57]

[26] Additionally, an application under the Wiretap Act must be approved at the highest levels of the US Department of Justice (DOJ) before it is authorized for submission to a judge.[58] The Wiretap Act requires federal investigative agencies to submit requests for the use of certain types of electronic surveillance (primarily non-consensual interceptions of wire and oral communications) to the DOJ for review and approval before those requests may be submitted for judicial review.[59] The US Attorney General is tasked with reviewing and approving these requests, but is also allowed to delegate that authority to a limited number of high-level DOJ officials, including Deputy Assistant Attorneys General for the Criminal Division. These officials review and approve or deny requests for wiretaps[60] and to install and monitor electronic bugs (e.g., microphones).[61]

[27] As is the case with the SCA, the Wiretap Act provides remedies to data subjects whose communications have been unlawfully intercepted by the US government. Remedies under the Wiretap Act are, as with the SCA, available to EU data subjects.[62] Where an individual has "intentionally" violated the Act,[63] a data subject may be entitled to "appropriate relief."`[64] Relief

---

[51] The Wiretap Act is codified as Title I of ECPA, 18 U.S.C. §§ 2510–22.
[52] 18 U.S.C. § 2518(3)(a).
[53] *Id.*
[54] *Id.* § 2518(3)(c).
[55] *Id.* § 2518(4)(d).
[56] *Id.* § 2518(5).
[57] *Id.* ("Every order . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter").
[58] *See* 18 U.S.C. § 2516(1).
[59] *Id.*
[60] *Id.* § 2510(1).
[61] *Id.* § 2501(2).
[62] *See id.* §§ 2510(6), 2510(11) (defining "person" and "aggrieved person" under the statute); *see also Suzlon Energy v. Microsoft*, 671 F.3d 726, 731 (9th Cir. 2011), http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf ("The ECPA protects the domestic communications of non-citizens."). Since The Wiretap Act is codified under ECPA, *Suzlon* likewise applies to available remedies under 18 U.S.C. § 2520.
[63] 18 U.S.C. § 2511(1)(a).
[64] 18 U.S.C. § 2520.

can include an injunction of the action if ongoing, monetary damages, and additional punitive damages where appropriate.[65]

4. Foreign Intelligence Surveillance Act

[28] The Foreign Intelligence Surveillance Act (FISA) provides individual remedies for data subjects against unlawful acts of individual government officers. If an individual officer conducts surveillance of a data subject without first obtaining statutory or Presidential authorization, misuses surveillance information, or unlawfully discloses surveillance information, that individual officer can be sued by the data subject in US court.[66] Authorizing statutes, such as Section 702 of FISA, provide additional restrictions and safeguards for surveillance activities. A data subject who succeeds in suing an individual for conducting unauthorized surveillance may receive actual damages of not less than $1,000 USD, statutory damages of $100 USD per day of unlawful surveillance, and the award of additional punitive damages and attorney's fees where appropriate.[67] As discussed in Chapter 5, the Foreign Intelligence Surveillance Court (FISC) has been diligent in policing agencies that attempt to circumvent its judicial orders, and conducts ongoing review of surveillance programs. Along with the existence of the individual statutory remedies, the FISC has made clear that failure to comply with its orders can result in the revocation of authorization for surveillance programs.[68] An aggrieved EU data subject may use the FISA cause of action as long as he or she is not a "foreign power" or an "agent of a foreign power."[69]

B. US Criminal Judicial Remedies

[29] In addition to allowing aggrieved individuals to bring civil suits against violators, the US DOJ can also bring criminal charges against any such violators under the SCA, ECPA, FISA, and the Privacy Act. Under the SCA, an individual who unlawfully accesses stored communications "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act" is subject to a criminal fine, up to five years imprisonment, or both for a first offense.[70] For subsequent offenses, the penalty increases to criminal fines, up to ten years imprisonment, or both.[71] In any other case, a first offense carries a penalty of criminal fine and/or imprisonment up to one year, and subsequent offenses carry a penalty of criminal fine and/or imprisonment up to five years.[72] If a person knowingly makes unlawful use of a pen register or trap/trace device can also face a penalty of criminal fines, up to one year imprisonment, or both.[73] Under ECPA, a person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or

---

[65] *Id.* §2520(b). Unlike the SCA, the Wiretap Act does not expressly grant a waiver of sovereign immunity for suits against US agencies, but rather allows for suit only against individual officers who have intentionally violated the Act. *Id.* § 2511(1).
[66] 50 U.S.C. §§ 1801, 1810.
[67] *Id.* § 1810. Note that the individual may receive either actual damages not less than $1,000 USD or $100 USD per day of surveillance, but not both.
[68] *Id.*
[69] 50 U.S.C. § 1801(a)-(b) (defining foreign power and agent of a foreign power).
[70] 18 U.S.C. § 2701(b)(1)(A).
[71] *Id.* § 2701(b)(1)(B).
[72] *Id.* § 2701(b)(2).
[73] 18 U.S.C. § 3121(d).

electronic communication" can face criminal fines, up to five years imprisonment, or both.[74] The same penalty applies to individuals who unlawfully use or disclose the contents of any wire, oral, or electronic communication.[75] Under FISA, a person who intentionally engages in unauthorized "electronic surveillance under color of law" or knowingly "discloses or uses information obtained under color of law by [unauthorized] electronic surveillance" can face a criminal fine, up to five years imprisonment, or both.[76] Under the Privacy Act, any officer or employee who uses his employment or official position to knowingly and willfully engage in prohibited disclosure of individually identifiable information "in any manner to any person or agency not entitled to receive" can be found guilty of a misdemeanor and fined up to $5,000.[77] These criminal penalties serve as an alternative means of redress for violations of a data subject's privacy rights. The US has strongly committed to effective enforcement of violations of privacy law, as demonstrated in the Judicial Redress Act, the Umbrella Agreement, and the Privacy Shield Framework.[78] Based on those commitments, the US DOJ would take any criminal-level violation of these laws seriously, as well as any request from the EU for criminal enforcement. In particular, the Ombudsman mechanism created by the Privacy Shield Framework demonstrates the US's commitment to cooperation with EU authorities regarding privacy violations.

[30] Along with the affirmative use of the criminal law against violations of privacy laws, I briefly discuss two areas where individuals, including EU citizens, have important rights in criminal prosecution. First is the exclusionary rule. As discussed elsewhere in my materials, the data subject has the ability in criminal cases to suppress unlawfully obtained evidence that the US government seeks to use in court.[79] US courts will not only bar illegally obtained evidence, but will also bar evidence acquired as a result of the illegal search or seizure.[80] If the suppression of illegally obtained evidence leaves the prosecutor without enough facts in evidence to meet the elements of the crime alleged, the case may then be dismissed.[81] Any objection to illegally obtained evidence during trial can later be appealed even if the accused is convicted, allowing for additional, independent judicial review of the government's actions.[82] These remedies are available to all persons facing criminal charges in US court, including EU persons.

---

[74] 18 U.S.C. §§ 2511(1)(a), 2511(4)(a).
[75] *Id.* § 2511(1).
[76] 50 U.S.C. §§ 1809(a), 1809(c).
[77] 5 U.S.C. § 552a(i)(1).
[78] *See* Council Decision (EU) No. 2016/920 of 20 May 2016 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, 2016 O.J. (L 154) 1; *see also* PRIVACY SHIELD FRAMEWORK, *Recourse, Enforcement and Liability*, https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY; Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2015).
[79] *See* Chapter 4; *see also* 18 U.S.C. § 2518(10)(a); *United States v. Warshak*, 631 F.3d 266, 282-89 (6th Cir. 2014) (noting that evidence acquired under the Stored Communications Act without a warrant is subject to the exclusionary rule).
[80] *Wong Sun v. United States*, 371 U.S. 471 (1963), https://scholar.google.com/scholar_case?case=13688369940584894086&hl=en&as_sdt=6&as_vis=1&oi=scholar.
[81] FED. R. CRIM. P. 29 ("After the government closes its evidence or after the close of all evidence, the court on the defendant's motion must enter a judgment of acquittal of any offense for which the evidence is insufficient to sustain a conviction.").
[82] FED. R. EVID. 103 (explaining how a party can preserve the right to appeal a ruling to admit or exclude evidence at trial).

[31] The Classified Information Procedures Act (CIPA) also provides a specific mechanism for allowing criminal defendants to access classified materials at trial that may be helpful to the defense.[83] As with other individual remedies available for individuals who are accused of a crime, CIPA protects the right of an individual to due process in a criminal proceeding. I discuss CIPA and its procedures in greater detail in Chapter 8 (Individual Remedies, Hostile Actors, and National Security Considerations).[84]

II. Non-Judicial Individual Remedies in the US against the US Government

[32] In addition to judicial remedies, there are important administrative, legislative, and public channels for data subjects to seek redress for privacy harms by the US government. This section examines specific avenues for such complaints and the relevant actions each entity may take in response to such a complaint. I highlight three such channels: the PCLOB; Congressional committees; and recourse to the free press and privacy-protective non-government organizations. Both US and EU persons can benefit from the ability to make complaints in these ways, and gain a multiplier effect as the agency, Congressional committee, or privacy advocacy organization takes up the cause.

A. The Privacy and Civil Liberties Oversight Board (PCLOB)

[33] The PCLOB, discussed in greater detail in Chapter 3, is an independent agency within the US government's executive branch with oversight authority over US intelligence practices, and the ability to respond to individual complaints. The PCLOB has extensive investigative powers, including access to necessary classified information. The PCLOB provides contact information to the public, and any person may submit concerns regarding US intelligence practices. The PCLOB has published lengthy reports on US intelligence procedures, including the numerous recommendations for reform of practices under Section 702, discussed in Chapter 3.[85] An EU data subject or DPA is free to contact the PCLOB and lodge a complaint or request for further investigations.

B. Congressional Committees

[34] The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence are discussed in greater detail in Chapter 3. Using their oversight authority, the Committees can investigate individual complaints from US and EU data subjects. These Committees were created to "oversee and make continuing studies of the intelligence activities and programs of the United States Government," and "provide vigilant legislative oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States."[86] As with the PCLOB, members of the committees

---

[83] 18 U.S.C. app. §§ 1-16.
[84] Chapter 8, Section IV ("US Criminal Proceedings under the Classified Information Procedures Act").
[85] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 134-148 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.
[86] 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.

and staff obtain top-secret clearances as necessary to conduct their oversight. Senate and House Judiciary committees play a similar oversight role for criminal law, as opposed to intelligence law. Individuals and DPAs can report their concerns to the relevant congressional committees and request follow-up investigations.

C. Individual Remedies through Public Press and Advocacy

[35] The free press of the US can serve as an important remedy for persons harmed by US surveillance. In contrast to the Official Secrets Acts in other countries, the First Amendment of the US Constitution has been interpreted to strictly protect the freedom of US journalists to report on national security issues such as surveillance. It similarly protects against overuse of defamation and libel claims by requiring strict proof for any such suit.[87] Complaints made to US reporters can be investigated, and those reporters enjoy significant protection from state censorship even where national security secrets are at issue. One such protection is that the US government may not engage in prior restraint of journalists, whether they are the New York Times or an independent journalist publishing online. [88] In other words, the US can respond to a published story but may not prevent the journalist from publishing at all. So, while an individual with a classified clearance may be guilty of a crime for sharing classified information with an unclassified party, the journalist is likely protected under the First Amendment for publishing any documents so acquired.[89]

[36] The US Supreme Court supported the ability of journalists to publish in *Bartnicki v. Vopper*, where the Court explained that this protection extends even to journalists who disclose illegally obtained or sourced information.[90] In *Bartnicki*, the Court examined what protection the First Amendment provides to speech that discloses the contents of an illegally intercepted communication.[91] The Court held that the First Amendment protects a journalist who receives and publishes unsolicited but illegally acquired information of public interest.[92]

---

[87] U.S CONST. amend. I, *New York Times Co. v. Sullivan*, 376 U.S. 254, 727 (1964) (requiring proof of actual malice "to award damages for libel in actions brought by public officials against critics of their official conduct").

[88] *See New York Times Co. v. United States*, 403 U.S. 713, 717 (1971) ("Both the history and language of the First Amendment support the view that the press must be left free to publish news, whatever the source, without censorship, injunctions, or prior restraints.") (Black, J., concurring).

[89] The US's Espionage Act prohibits the communication, publication, or transmission of classified information related to communication intelligence activities. 18 U.S.C. § 798. Scholars believe the First Amendment's prohibition of prior restraint would bar enforcement of the Espionage Act against journalists and other independent speakers *See* Patricia L. Bellia, *Wikileaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1526 (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033207 (concluding that the Pentagon Papers case used the possibility of criminal responsibility and an ethical responsibility to prevent harm to influence how publishers used the Pentagon papers); Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 234 (2007), https://ssrn.com/abstract=963998 (noting that while the Espionage Act could criminalize some journalist activities, the First Amendment "could be seen as conferring at least *some* minimal privilege on reporters who are, in good faith, attempting to uncover illicit governmental activity").

[90] *Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001) https://supreme.justia.com/cases/federal/us/532/514/case.html ("We think it's clear that parallel reasoning requires the conclusion that a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern.")

[91] *Id.* at 517.

[92] *Id.* at 535.

[37] In contrast, under EU Member State laws, it would appear that the facts of *Bartnicki* may have left the New York Times guilty under an Official Secrets Act.[93] Under the UK Official Secrets Act, for instance, a person "into whose possession the [protected] information, document or article has come is guilty of an offence if he discloses it without lawful authority knowing, or having reasonable cause to believe, that it is protected against disclosure"[94] by the Act if "the disclosure . . . is damaging, and he makes it knowing, or having reasonable cause to believe, that it would be damaging."[95] Likewise, under Irish law "[a] person shall not communicate any official information to any other person unless he is duly authorized to do so or does so in the course of and in accordance with his duties as the holder of a public office or when it is his duty in the Interest of the State to communicate it."[96] In either case, there is not the same level of protection or defense for a newspaper publishing state secrets that may be in the public interest but may also be damaging or against the interest of the State.

[38] This means that a US journalist would be able to respond directly to complaints by EU persons, affording a path of action for aggrieved individuals. Major US publications such as the New York Times and the Washington Post published disclosures of classified information that came from Edward Snowden. US publications similarly are willing to publish information from EU persons. EU persons' redress to the US press can have direct effects, such as the government canceling a program, and indirect effects, such as helping lay the groundwork for legislation eventually enacted in Congress.[97] Since the press can use classified information in making these claims, it is more difficult for the US to ignore well-sourced journalism of this type.

[39] Along with going directly to the press, individuals can directly petition companies to report their own sharing of data in response to national security and law enforcement requests. As discussed in the Chapter 3, companies today are publishing detailed "transparency reports" about the number and type of government requests for personal data.[98] The Open Technology Institute has also provided a "Transparency Reporting Toolkit" to better assist companies in generating these reports to share relevant information as permitted under US law.[99] The Privacy Shield Framework explicitly permits participating organizations to provide transparency reports on lawful

---

[93] *See* Official Secrets Act 1989, c. 6, § 5 (U.K.), http://www.legislation.gov.uk/ukpga/1989/6/pdfs/ukpga_19890006_en.pdf, Official Secrets Act 1963 (Act. No. 1/1963) (Ir.), http://www.irishstatutebook.ie/eli/1963/act/1/enacted/en/print.html.

[94] *See* Official Secrets Act 1989, c. 6, § 5(2) (U.K.), http://www.legislation.gov.uk/ukpga/1989/6/pdfs/ukpga_19890006_en.pdf

[95] *Id.* § 5(3).

[96] Official Secrets Act 1963, § 4 (Act. No. 1/1963) (Ir.), http://www.irishstatutebook.ie/eli/1963/act/1/enacted/en/print.html.

[97] *See The Watergate Story*, WASH. POST SPECIAL REPORTS, http://www.washingtonpost.com/wp-srv/politics/special/watergate/ (reporting on how the publication of the Pentagon Papers led, in part, to the cessation of President Nixon's taping policies and his eventual impeachment). There is little doubt, in my view, that the disclosures by Edward Snowden through the press played an important causal role in the reforms in the US since 2013.

[98] *See generally* RYAN BUDISH, ET AL., NEW AMERICA, OPEN TECHNOLOGY INSTITUTE, THE TRANSPARENCY REPORTING TOOLKIT (Mar. 31, 2016), https://www.newamerica.org/oti/policy-papers/the-transparency-reporting-toolkit/ (providing guidance on transparency reporting best practices for companies).

[99] *Id.*

access requests from the US government.[100] Making this data public allows more individuals and the press to be aware of the scope of lawful access taking place and to petition for restraint or cancellation of programs where appropriate.

[40] Non-governmental privacy advocate organizations in the US use their expertise and resources to pursue systemic change and recourse on behalf of aggrieved individuals.[101] The Electronic Privacy Information Center (EPIC), for example, which is participating in the current proceeding, undertakes numerous privacy protective activities, including petitions to the Federal Trade Commission regarding individual complaints.[102] The Center for Democracy and Technology engages in numerous privacy related activities, including publications, filing of official comments, and advocacy before Congress and executive agencies on issues such as secrecy and surveillance.[103] The American Civil Liberties Union, Electronic Frontier Foundation, Open Technology Institute, and many other non-governmental organizations conduct similar efforts, including accessing and compiling government documents through the Freedom of Information Act.[104] An individual concerned about his or her privacy rights can petition to any or all of these organizations, who can then work independently or in concert to bring their resources to bear on remedying an individual wrong or influencing changes in US policies and procedures.[105]

---

[100] *See* US DEP'T OF COMMERCE, PRIVACY SHIELD FRAMEWORK, *Access Requests by Public Authorities* (2016), https://www.privacyshield.gov/article?id=16-Access-Requests-by-Public-Authorities.

[101] *See, e.g.*, ELECTRONIC PRIVACY INFORMATION CENTER, *EPIC Administrative Procedure Act (APA) Comments*, EPIC.ORG, https://epic.org/apa/comments/.

[102] *Id.*

[103] *See* CENTER FOR DEMOCRACY & TECHNOLOGY, *About CDT*, https://cdt.org/about/.

[104] *Section 215 Documents*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/foia-collection/section-215-documents.

[105] In connection with press-related remedies, The US Freedom of Information Act (FOIA) is sometimes cited as a potential individual remedy, as it generally permits individuals to require the US federal government to disclose information in its possession. *See* 5 U.S.C. § 552(a). FOIA will likely not result in access, however, when the information sought is classified national security information. FOIA does not require US agencies to disclose such information. *Id.* § 552(b).

FOIA's national-security exclusion is longstanding and well known. For example, the EU Commission's Privacy Shield Adequacy Decision noted that FOIA will not permit individuals to obtain data from US intelligence agencies because such "agencies may withhold . . . classified national security information." 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. 114, 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.

In several EU Member States, freedom-of-information statutes similarly exclude classified national security information from access rights. *See, e.g.*, (1) France: CODE DES RELATIONS ENTRE LE PUBLIC ET L'ADMINISTRATION [CODE OF RELATIONS BETWEEN THE PUBLIC AND THE ADMINISTRATION], Art. L. 311-5 (excluding documents that may compromise defense secrets, foreign relations, the security of the State, or public safety from access rights), (in French) https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000031366350&idArticle=LEGIARTI000031367708; (2) Germany: Informationsfreiheitsgesetz [Freedom of Information Act], § 3 (excluding information that "may have detrimental effects on" international relations, military interests, or internal or external security interests from access rights), (in English) https://www.gesetze-im-internet.de/englisch_ifg/englisch_ifg.html#p0016; (3) Ireland: Freedom of Information Act 2014, (Act. No. 30/2014), § 33 ("A head may refuse to grant an FOI request . . . if . . . access to [a record] could reasonably be expected to affect adversely (a) the security of the State, (b) the defence of the State . . . (d) the international relations of the State."), http://www.irishstatutebook.ie/eli/2014/act/30/enacted/en/print#sec33.

[41] Lawyers sometimes assume that legal action is the most effective way to remedy a problem and effect change. In the discussion here, I highlight the crucial ways that remedies occur in the US through a free press, advocacy to the companies about their practices, and the efforts of non-governmental organizations. The role of the press and non-governmental organizations is often substantial in the US for surveillance and privacy issues. In my view, a fair assessment of the checks and balances that exist against surveillance abuse should include consideration of the role of the free press and public advocacy.

III. Additional US Privacy Remedies under Federal Law

[42] This Section first examines individual remedies against US companies, such as service providers of webmail and social networks, should they improperly disclose information to the US government about customers. It then examines privacy enforcement by federal administrative agencies, including the FTC and FCC.

A. Privacy Remedies against Service Providers

[43] Individual remedies are available against US companies, such as service providers of webmail and social networks, should they engage in activities that violate either relevant state or federal privacy laws or their own public privacy policies.[106] Using its law enforcement and foreign intelligence authorities, the US government can seek to compel the production of personal data from a US company, or compel the aid of a company in conducting wiretaps or surveillance.[107] These service providers have strong incentives to follow the law and their stated company policies. Violations can result in lawsuits against the service provider, as well as business harms if consumers lose trust in the ability of the companies to safeguard communications and other personal data. Lawsuits are notably available for violation of the Stored Communication Act or Wiretap Act.

[44] In light of the legal and business risks that face companies that violate law and policy, companies have considerable incentive to comply with applicable laws and policies. Compliance, in turn, means companies have reason to scrutinize government requests for information. Major Internet companies have become even stricter in this area since 2013 in the face of government requests for data. For instance, companies have adopted strong encryption in many new settings, protecting communications from wiretaps and other government efforts to access data.[108] In addition, major companies have increasingly challenged US government data requests in court,

---

[106] Although I use the term "service provider" in the text here to describe webmail and social network services, the statutory definition of "service provider" in US law is quite broad, as described in Chapter 9.

[107] *See* Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1001 (requiring telecommunications carriers to make their equipment capable of enabling government wiretaps), 18 U.S.C. § 2703(a) (detailing how US law enforcement can compel the production of individuals' stored content).

[108] The increased prevalence of strong encryption has been a topic of several of my writings, including Peter Swire & Justin Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, N.Y.U. ANN. SURVEY AM. L. (forthcoming 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728478.

including in the 2015 *Microsoft Ireland* case.[109] A suit by individuals against a non-compliant company can pay at least statutory damages and attorney's fees. In addition, under the liberal American rules for discovery in court cases, individual suits can become an engine for generating more information that is critical of the company and the government request. In short, the risk of such individual suits shape what information companies are willing to provide the government.

1. Stored Communications Act

[45] Just as the SCA provides a cause of action for individuals against the US government, so too does it allow for civil actions against private companies that unlawfully disclose personal data.[110] Under the SCA, a data subject can obtain preliminary relief (e.g., injunctions) where appropriate, actual damages in an amount of no less than $1,000 USD (with an option for punitive damages where the violation was "willful"). Claimants can also recover court costs and attorney's fees, where appropriate. If a company shares data in good faith reliance on "a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization" then it cannot be found liable for any damages. Here again, the law allows for the systemic safeguards present in obtaining a valid instrument, but still allows a suit to continue if those checks are allegedly improperly circumvented. Just as noted earlier, the SCA allows any aggrieved person, including an EU data subject, to exercise its right of action.[111]

[46] In 2006, USA Today reported that telephone companies had supplied the US government with "the phone call records of tens of millions of Americans."[112] With a co-author, I published an article explaining how telecommunications companies who had shared stored phone records with the NSA could be liable for large amounts of statutory damages.[113] Since the providers appeared to have shared information with the NSA absent the required legal authority (e.g., a warrant) those companies that shared their subscribers' information could have been held liable for at least $1,000 USD per customer. The statutory minimum damage of $1,000 can be particularly important where the violations affect many individuals. For the records of fifty million individuals, that would mean liability of a staggering $50 billion. In 2008, Congress provided immunity to suit against the telephone companies for providing these records. In retrospect, it appears that the records were provided under a judicial order for the Section 215 telephone metadata program. The continued existence of the $1,000 USD per person statutory damages provides a powerful reason for both the government and service providers to comply with the Stored Communications Act.

---

[109] *Microsoft v. United States*, No. 14-2985, 2016 U.S. App. LEXIS 12926, at *46–49 (2d Cir. July 14, 2016), http://www.ca2.uscourts.gov/decisions/isysquery/2ec5a1b3-97ee-47c4-9224-1ea5b86ebbd4/6/doc/14-2985_complete_opn.pdf.

[110] 18 U.S.C. § 2707.

[111] *Id.* § 2707(a); *Suzlon Energy v. Microsoft*, 671 F.3d 726, 730 (9th Cir. 2011), http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf.

[112] Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY (May 11, 2006, 10:38 PM), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[113] Peter Swire, *Questions and Answers on Potential Telco Liability*, THINK PROGRESS (May 12, 2006), https://thinkprogress.org/questions-and-answers-on-potential-telco-liability-e5fa4bdd4c0d#.1qokc850w.

2. Wiretap Act

[47] The Wiretap Act provides a right of action against any person or entity, other than the US government, that violates the statute in intercepting, disclosing, or using surveillance data.[114] Barring an exception, the interception of communications is a criminal offense.[115] Exceptions to the rule are narrow. For example, interception is permitted if there is valid consent.[116] Another exception exists for interception done "in the ordinary course of business."[117] For example, routine call monitoring in a call center would qualify as exempted interception in the normal course of business.[118] An employer listening to an employee's personal call, however, would not fall under the exemption and would therefore still constitute a criminal interception under the Act.[119]

[48] A person whose communications are unlawfully intercepted may also bring suit against the intercepting party.[120] If the suit succeeds, then the individual is eligible for preliminary relief where appropriate, including enjoining ongoing surveillance, reasonable attorney's fees and costs if appropriate, and monetary damages.[121] These damages can either be the sum of actual damages caused by the violation or statutory damages. Statutory damages are determined as the greater of either $100 USD per day of the ongoing violation or $10,000 USD.[122] As with the SCA, companies can again rely on documents compelling cooperation with the US government as a defense in any action under the Wiretap Act.[123] Also like the SCA, an EU data subject can directly bring suits against companies for violation of the Wiretap Act.[124]

B. Enforcement by Federal Administrative Agencies

[49] I next discuss five major administrative agencies in the US that also serve as privacy enforcers: The FTC, the FCC, the Consumer Financial Protection Bureau (CFPB), the Securities and Exchange Commission (SEC), and the Department of Health and Human Services (HHS). As shown in my textbook on US private-sector privacy law, other federal agencies also play roles in privacy enforcement, usually depending on the sector that each agency oversees.

---

[114] *See* SWIRE & AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 142.
[115] *Id.*
[116] *Id.* Note that the required consent can vary depending on the state. The Wiretap Act itself allows for a single party's consent, but some states require all parties to a call to consent to the interception. In practice, this means many companies will use a notification, such as "This call may be recorded for quality assurance purposes" to ensure all parties have an opportunity to disconnect or object.
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] 50 U.S.C. § 1810.
[122] *Id.*
[123] *Id.* § 1810(a).
[124] 18 U.S.C. § 2510(6) (defining "person" under the statute without restrictions based on citizenship), http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2703&num=0&edition=prelim; *see also Suzlon Energy v. Microsoft*, 671 F.3d 726, 730 (9th Cir. 2011), http://cdn.ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf ("Thus, the Court remains firm in its initial finding that the ECPA unambiguously applies to foreign citizens.").

These administrative agencies do not themselves bring actions against intelligence agencies. They can be important, however, because they can bring actions against companies that fail to comply with applicable law or company privacy policies, such as when the companies improperly provide electronic communications to the government.

1. The Federal Trade Commission (FTC)

[50] The FTC is tasked with regulating and enforcing actions in US commerce for the protection of consumers and the public welfare.[125] In 1938, the FTC's mission was expanded from its original mission to enforce antitrust laws to include protecting consumers generally.[126] The FTC exists independently from other executive agencies, meaning it is not under the direct control of the US President.[127] Instead, the Commission is headed by a chairman and four other commissioners who govern its activities, no more than three of whom can be from the same political party.[128]

[51] The FTC's authority comes from the Federal Trade Commission Act (FTC Act), which includes arguably the "single most important piece of US privacy law":[129] "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[130] While the statute does not explicitly mention data privacy, US law today has thoroughly established that the prohibition against unfair and deceptive practices applies to privacy and information security.[131] Unfair and deceptive practices can include company actions that violate the company's privacy statement,[132] inadvertent sharing of subscriber email addresses,[133] and misleading statements about the level of data security present in a website or Internet service.[134] Over time, the FTC's role as privacy enforcer was expanded by Congress to include regulatory and enforcement authority over misuse of children's data[135] and spam email practices.[136]

[52] FTC enforcement investigations are often in response to consumer complaints made directly to the agency, press reports, complaints from business competitors, or from internal research at the FTC.[137] The FTC has broad authority to investigate these claims, including the ability to subpoena witnesses, make civil investigative demands, and require companies to submit written reports under oath.[138] Once the FTC investigation is complete, the Commission decides if it will issue a legal complaint to begin an administrative trial before an Administrative Law Judge, whose

---

[125] *See* FEDERAL TRADE COMMISSION, *About the FTC*, https://www.ftc.gov/about-ftc.
[126] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 14.
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] 15 U.S.C. § 45.
[131] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 14.
[132] *Id.* at 17 (discussing *In the Matter of GeoCities, Inc.*).
[133] *Id.* (discussing *In the Matter of Eli Lilly & Co.*).
[134] *Id.* (discussing *In the Matter of Microsoft Corp.*).
[135] *Id.* at 14 (discussing the FTC's authority under the Children's Online Privacy Protection Act).
[136] *Id.* (discussing the FTC's authority under the Controlling the Assault of Non-Solicited Pornography and Marketing Act).
[137] *Id.* at 15.
[138] *Id.*

decision can be appealed to a federal district court in the US.[139] Companies found to engage in unfair or deceptive practices can be fined up to $16,000 USD per violation, and the FTC can seek damages to compensate those harmed by the unlawful activity.[140] In practice, the FTC often settles these enforcement actions through consent decrees and accompanying consent orders.[141] Consent decrees are public documents which bind a company to abide by changes to its business practices.[142] Consent decrees often require the company to prove compliance over time and to inform all related persons of obligations under the consent decree.[143] Companies under a consent decree must also inform the FTC if any changes in company operations will affect the company's ability to abide by the consent degree's terms.[144] These decrees also typically require periodic outside audits or reviews of company practices and may even require a company to adopt and implement a comprehensive privacy program.[145] If a company violates a consent decree, the FTC can bring another enforcement action in federal district court to seek additional fines as well as injunctions and other forms of relief.[146]

[53] These actions not only provide a remedy for unfair or deceptive actions but also function as a de facto common law of privacy norms and best practices. Professors Daniel J. Solove & Woodrow Hartzog's article, *The FTC and the New Common Law of Privacy*, examines FTC complaints, consent decrees, reports, and other materials and how these document can "impos[e] certain default standards" for privacy.[147] Solove and Hartzog argue "that today FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States."[148] They also point out that while the US's sectoral approach can appear to leave large areas unregulated, the FTC actually regulates those parts through its "sprawling jurisdiction to enforce privacy."[149] To illustrate this point, the following examples are some of the FTC's more notable enforcement actions from the past ten years:

1. ***United States v. Google, Inc.*:** The FTC entered into a consent decree with Google resulting in a $22,500,000 USD civil penalty for failing to comply with a previous consent order restricting Google's ability to make representations about the control users had over their information and its collection.[150] In this case, the FTC fined Google for overriding default cookie collection settings in Safari browsers. Google remained under control of the previous consent order,

---

[139] *Id.*
[140] *Id.*
[141] *See id.*; *see also Cases and Proceedings*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/enforcement/cases-proceedings.
[142] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 15.
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583, 676 (2014) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.
[148] *Id.* at 587.
[149] *Id.* at 588.
[150] *See United States v. Google Inc.*, No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012) (order), http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121120googleorder.pdf.

and was additionally required to report on their continued maintenance after the incident.

2. ***United States v. Xanga.com, Inc.*:** The FTC entered into a consent decree with Xanga, Inc. resulting in a $1,000,000 USD civil penalty.[151] The FTC alleged that Xanga, Inc. inadequately prevented children under the age of 13 from registering for an account and sharing personal information and failed to provide proper notice of their practice. Xanga, Inc. was also required to stop violating the Children's Online Privacy Protection Act (COPPA), provide conspicuous notice of its practices, and delete all information collected from children.

3. ***United States v. Sony BMG Music Entertainment*:** The FTC entered into a consent decree with Sony resulting in a $1,000,000 USD civil penalty.[152] The FTC alleged that, despite Sony's privacy policy's representations that children under 13 were not able to register for Sony sites, those sites accepted registrations with an entered age under 13. Since parents of these children were not notified nor did the parents provide verifiable consent, the FTC alleged violations under COPPA. In addition to the civil penalty, Sony's consent decree required that Sony delete all information that was unlawfully collected, provide prominent notice about usage and collection of children's data on their website, and provide parents of children under 13 using Sony sites with actual notice of the collection and use of children's personal information.

4. ***United States v. Path, Inc.*:** The FTC entered into a consent decree with Path, Inc., resulting in an $800,000 USD fine and twenty year commitment to biennial assessments and reports.[153] Path was charged with misleading customers concerning information use, failing to obtain consent to data collection from a user's address book, and collecting personal information from children under the age of 13 without verifiable parental consent in violation of COPPA.

[54] Notably, as part of the US's participation in the Privacy Shield Framework, the FTC has committed to assistance in four areas: "(1) referral prioritization and investigations; (2) addressing false or deceptive Privacy Shield membership claims; (3) continued order monitoring; and (4) enhanced engagement and enforcement cooperation with EU DPAs."[154] This assistance includes information sharing and investigative assistance, including sharing information obtained in connection with an FTC investigation, issuing compulsory process on behalf of an EU DPA

[151] *See United States v. Xanga.com, Inc.*, No. 06 CV 6853 (S.D.N.Y. Sep. 12, 2006), https://www.ftc.gov/sites/default/files/documents/cases/2006/09/xangaconsentdecree_image.pdf.
[152] *See United States v. Sony BMG Music Entertainment*, No. 08 Civ. 10730 (S.D.N.Y. Dec. 15, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211consentp0823071.pdf.
[153] *See United States v. Path, Inc.*, No. 3:13-CV-00448-RS (N.D. Cal. Feb. 8, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.
[154] Letter dated July 7, 2016 from Edith Ramirez, Chairwoman, FTC, to Věra Jourová, Comm'r for Justice, Consumers and Gender Equality, European Commission 2, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0v.

conducting its own investigation, and seeking oral testimony from witnesses or defendant in connection with an EU DPA's enforcement proceeding.[155] To assist in these commitments, the FTC will create a standardized referral process and provide guidance to EU Member States on the type of information that would best assist the FTC in its inquiry following a referral.[156] The FTC has also committed to exchanging information on referrals with referring enforcement authorities and to working closely with EU DPAs in providing enforcement assistance.[157]

2. The Federal Communications Commission (FCC)

[55] The FCC is responsible for regulating and enforcing rules for "interstate and international communications by radio, television, wire, satellite and cable" in the US.[158] Like the FTC, the FCC is independent from the President's control. While the FTC focuses primarily on enforcement actions,[159] the FCC both issues legal regulations for industries under its oversight and enforces telecommunications law and regulations, including for privacy.[160] The FCC's primary privacy oversight function traditionally centered around rules for customer proprietary network information (CPNI). Under the Telecommunications Act and an accompanying FCC rule, telecommunications carriers were restricted in how they could access, use, and disclose their subscribers CPNI. CPNI includes subscription information, services used, network and billing information, phone features and capabilities, and more.[161] Today, a telecommunications carrier that shares a subscriber's CPNI without the express, opt-in consent of the subscriber is subject to enforcement and fines by the FCC.[162] The FCC has vigorously pursued enforcement of violations of these rules, including a $1,300,000 USD settlement with Verizon Wireless over the use of "supercookies."[163] Like the FTC, the FCC may begin an investigation on its own volition or in response to petitions from outside parties, including EU data subjects and DPAs, though it is not required to investigate each complaint.

[56] Examples of recent privacy enforcement from the FCC include:

1. ***In the Matter of AT&T Services, Inc.*:** In this case, the FCC entered into a consent decree with AT&T requiring a civil penalty of $25,000,000 USD.[164] The FCC's investigation alleged the unauthorized disclosure of approximately 280,000 customer names, social security numbers, and other CPNI.[165] Specifically, the FCC alleged that employees at AT&T call centers in Central and South America were able to access CPNI while obtaining other personal

[155] *Id.* at 6.
[156] *Id*.
[157] *Id*.
[158] *See* FEDERAL COMMUNICATIONS COMMISSION, *What We Do*, https://www.fcc.gov/about-fcc/what-we-do.
[159] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 14-15.
[160] *See What We Do*, *supra* note 160.
[161] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 100.
[162] *Id*.
[163] *In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, FCC Rcd DA 16-242 (Mar. 7, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DA-16-242A1.pdf.
[164] *In the Matter of AT&T Services, Inc.*, FCC Rcd DA 15-399, 1 (Apr. 8, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-399A1.pdf.
[165] *Id.* at 4.

information used to unlock stolen cell phones.[166] AT&T was also required to notify all customers whose accounts were improperly accessed, appoint a senior compliance manager, conduct a privacy risk assessment, implement an information security program, prepare an appropriate compliance manual, and regularly train employees on the company's privacy policies and applicable privacy laws.[167]

2. ***In the Matter of Verizon*:** In this case, the FCC entered into a consent decree with Verizon Wireless requiring a fine of $7,400,000 USD.[168] The FCC's investigation alleged that Verizon had failed to notify customers of their privacy and opt-out rights before using personal information for marketing purposes in violation of the CPNI requirements.[169] Verizon was also required to notify customer of their opt-out rights on every bill for three years from the date of the order, put systems in place to monitor and test its billing and opt-out process, and develop and implement a three-year compliance plan including annual compliance reports.[170]

3. ***In the Matter of TerraCom, Inc. and YourTel America, Inc.*:** In this case, the FCC entered into a consent decree with TerraCom and YourTel, requiring a fine of $3,500,000 USD.[171] The FCC alleged that the companies failed to protect the confidentiality of customer proprietary information provided for demonstrating eligibility for the Lifeline program, and engaged in unjust and unreasonable practices in failing to employ reasonable data security practices to protect customers' proprietary information.[172] The FCC further alleged that the companies misrepresented that they employed reasonable data security practices to protect customer proprietary information in their respective privacy statements.[173]

[57] In 2015, the FCC reclassified Internet service providers as a covered telecommunications company, moving them from the FTC's jurisdiction to the FCC's jurisdiction.[174] Since then, the FCC has engaged in the formal process for a new regulation governing privacy for broadband Internet service providers.[175] On October 27, 2016, the FCC adopted its final privacy rule for

---

[166] *Id*.
[167] *Id.* at 6-13.
[168] *In the Matter of Verizon Compliance with the Commission's Rules and Regulations Governing Customer Proprietary Network Information*, FCC Rcd DA 14-1251, *1 (Sept. 3, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1251A1_Rcd.pdf.
[169] *Id.*at *5.
[170] *Id.* at *6-9.
[171] *In the Matter of TerraCom, Inc., and YourTel America, Inc.*, FCC Rcd DA 15-776, *19 (July 9, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-776A1_Rcd.pdf.
[172] *Id.* at *1.
[173] *Id*.
[174] *See Protecting and Promoting the Open Internet*, 80 Fed. Reg. 19737 (Apr. 13, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-04-13/pdf/2015-07841.pdf.
[175] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 81 Fed. Reg. 23360 (Apr. 20, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-04-20/pdf/2016-08458.pdf.

broadband Internet service providers, requiring affirmative opt-in consent before using or sharing any sensitive information, such as geolocation data, financial information, health information, children's information, web browsing history, app usage history, and the content of communications.[176]

3. The Consumer Financial Protection Bureau (CFPB)

[58] In 2010, the CFPB was created under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).[177] The CFPB is responsible for overseeing relationships between consumers and the providers of financial products and services.[178] Under Dodd-Frank, the CFPB has broad authority to examine, regulate, and enforce actions of business that provide financial services and products.[179] The CFPB is also able to make rules under other existing financial privacy acts, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Fair Debt Collection Practices Act.[180] Like the FTC, the CFPB can bring enforcement actions against businesses under its oversight for unfair and deceptive practices.[181] The CFPB is also authorized to enforce against "abusive acts and practices," including materially interfering with a consumer's ability to understand a term or condition of a consumer financial product; taking unreasonable advantage of a lack of understanding by the consumer of material risks, costs, and conditions; and taking unreasonable advantage of a consumer's inability to protect its interests.[182]

[59] The CFPB is authorized to conduct investigations, issue subpoenas, hold hearings, and commence civil actions against offenders.[183] For violations of federal consumer privacy law, a company can face of $5,000 USD per day.[184] If the company's violation of law was reckless, they can instead be held liable for $25,000 USD per day.[185] Finally, if the company knowingly violated federal consumer protection law, companies can face fines of up to $1,000,000 USD per day. The CFPB can also seek to impose "limits on the activities or functions" of the offender.[186] While the CFPB has not engaged in prominent privacy enforcement to date, it is worth examining its actions as a consumer protection enforcer generally as evidence of how it carries out its enforcement authority under Dodd-Frank and other Acts.

[60] As an example of strong enforcement by the CFPB, in 2014, the Board entered into a consent order with GE Capital Retail Bank, requiring payment of an estimated $225,000,000 USD in relief

---

[176] *See* Press Release, Federal Communications Commission, FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency, and Security for their Personal Data (Oct. 27, 2016) http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1027/DOC-341937A1.pdf.
[177] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 71.
[178] *Id.*
[179] *Id.*
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.* at 72.
[184] *Id.*
[185] *Id.*
[186] Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, § 1055(a)(2)(G), 124 Stat. 1376, https://www.sec.gov/about/laws/wallstreetreform-cpa.pdf.

to consumers allegedly harmed by illegal and discriminatory credit card practices.[187] The CFPB found two of GE Capital's promotions were discriminatory in not offering settlement and statement credit offers to individuals who preferred to communicate in Spanish or had a mailing address in Puerto Rico, even if the individual otherwise met the program's requirements.[188] In addition to the money GE Capital was required to reimburse to harmed consumers, GE Capital was required to end its deceptive practices and illegal discrimination and to notify credit reporting agencies of updated information. GE Capital was also required to pay an additional $3,500,000 USD penalty for its deceptive and unfair practices.

4. The Securities and Exchange Commission (SEC)

[61] Under the Securities Act, the SEC is empowered "to protect investors; maintain fair, orderly, and efficient markets, and facilitate capital formation."[189] Like the FCC, the SEC may also issue appropriate regulations and enforce against companies under its oversight that violate these laws and regulation.[190] In 2000, along with the other financial services regulatory agencies, the SEC adopted Regulation S-P on the Privacy of Consumer Financial Information.[191] Under the regulation, companies are required to provide adequate notice to their customers about privacy policies and practices, are restricted in how they may disclose nonpublic personal information about consumers to nonaffiliated third parties, and must provide a method for consumers to opt-out of any disclosure of their nonpublic personal information.[192] The regulation also includes a requirement that covered companies must safeguard customer records and information.[193]

[62] Examples of recent enforcement of these rules include:

1. ***In the Matter of Morgan Stanley Smith Barney, LLC*:** In this case, the SEC settled allegations of failure to protect consumer information, some of which was hacked and sold online, resulting in a $1,000,000 USD penalty.[194] The SEC's order found that Morgan Stanley had failed to adopt written policies and procedures to reasonably protect customer data.[195] The SEC further sanctioned the individual employee who downloaded and transferred confidential data to

[187] CFPB Consent Order, *In the Matter of Synchrony Bank, f/k/a GE Capital Retail Bank* (Jun. 19, 2014), http://files.consumerfinance.gov/f/201406_cfpb_consent-order_synchronybank.pdf.
[188] *Id.*
[189] *See About the SEC*, SEC, https://www.sec.gov/about.shtml.
[190] *See* The Securities Act § 19(a), 15 U.S.C. § 77s (granting the Commission authority to issue regulations and enforce violations under the Act), https://www.sec.gov/about/laws/sa33.pdf.
[191] SEC Final Rule: Privacy of Consumer Financial Information (Regulation S-P), 17 C.F.R. § 248, https://www.sec.gov/rules/final/34-42974.htm.
[192] *Id.* § 248.1.
[193] *Id.* § 248.30.
[194] *In the Matter of Morgan Stanley Smith Barney LLC*, File No. 3-17280, 6 (Jun. 8, 2016), https://www.sec.gov/litigation/admin/2016/34-78021.pdf.
[195] *Id.*

his personal server, and he was criminally convicted for his actions and received a sentence of 36 months' probation and a $600,000 USD restitution order.[196]

2. ***In the Matter of R.T. Jones Capital Equities Management, Inc.*:** In 2015, the SEC brought an enforcement action against an investment adviser for failing to properly protect its clients' personal information prior to a data breach.[197] Here, the adviser had failed to properly adopt written policies and procedures to protect its customer records and information for a 4-year period. The adviser settled with the SEC, agreeing to cease and desist from committing or causing future violations of the rule, and to pay a $75,000 USD fine.[198] As with an FTC consent decree, if the adviser were to fail to abide by the requirements of the settlement, it could be brought back into court to face additional penalties.[199]

[63] Safeguarding personal information is an essential element of privacy protection, and these recent cases highlight the SEC's interest in enforcement in this area.

5. The Department of Health and Human Services (DHHS)

[64] The approximately 17 percent of the US economy devoted to health care is governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.[200] In my role as Chief Counselor for Privacy, I was the White House coordinator of the proposed HIPAA Privacy Rule in 1999, and the final issue published in 2000. The rule was modified in 2003, and additional modifications were included in the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and the regulations implementing that Act.

[65] The HIPAA Privacy Rule creates a comprehensive system for protecting the privacy of individual's medical information, including requirements for privacy notices, authorizations for the use and disclosure of protected health information (PHI), limits to only use and disclose PHI to the minimum extent necessary, individual access and accounting rights, and security safeguards.[201]

[66] Within the HHS, the Office for Civil Rights (OCR) leads a large-scale enforcement program. OCR receives numerous complaints each year, and as of September 30, 2016, has resolved a total of 137,861 HIPAA complaints, with 39 such cases settled for a total of $45,889,200

---

[196] Press Release, SEC, Morgan Stanley Failed to Safeguard Customer Data, (Jun. 8, 2016), https://www.sec.gov/news/pressrelease/2016-112.html.
[197] Press Release, SEC, SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to the Breach, (Sep. 22, 2015), https://www.sec.gov/news/pressrelease/2015-202.html.
[198] *Id.*
[199] *See* 15 U.S.C. § 77i (explaining the procedure for having a Court review, and subsequently enter into force, any cease and desist or other order issued by the SEC), https://www.sec.gov/about/laws/sa33.pdf.
[200] *See* Health Insurance Portability and Accountability Act Privacy Rule, 45 C.F.R. § 160, https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/content-detail.html; Health Expenditure, Total (% of GDP), The World Bank, http://data.worldbank.org/indicator/SH.XPD.TOTL.ZS.
[201] *See* SWIRE AND AHMAD, *supra* note 1, at 48.

USD in civil money penalties.[202] In 15,746 cases, OCR provided early intervention and technical assistance to resolve the issue without the need for an investigation.[203] In 2014 alone, OCR investigated and resolved a total of 17,748 complaints.[204] OCR performs a combination of investigations of complaints and compliance reviews to determine where enforcement is needed.[205] If OCR reviews and accepts a complaint for investigation it will notify the filer and the cover entity named in the complaint to begin the investigation.[206] Covered entities are required by law to cooperate with these investigations.[207] Once the investigation is complete, OCR reviews the evidence gathered to determine whether the covered entity violated the Privacy or Security Rule.[208] If the covered entity was not in compliance with the rules, OCR may obtain voluntary compliance, corrective action, or a resolution agreement.[209] OCR may also impose a penalty between $100 USD and $50,000 USD /per violation, with a calendar year cap of $1,500,000 USD.[210] OCR publishes statistics on complaints and enforcement actions, which show an increasing trend in the number of total complaints resolved with 17,748 total resolutions in 2014 up from 14,293 in 2013, and less than 10,000 per year between 2004 and 2012.[211]

[67] In addition to investigations based on complaints, OCR conducts audits of covered entities to ensure HIPAA compliance.[212] OCR is currently developing a new audit program to better assess HIPAA compliance, identify best practices, discover risks and vulnerabilities, and address problems prior to a breach of data.[213] OCR is overseeing on-site auditing of a wide variety of covered entities and business associates in order to sample criteria across the spectrum of covered entities.[214]

[68] In 2003, HHS also issued a final version of the HIPAA Security Rule, which reinforces the safeguards in the Privacy Rule. The Security Rule establishing minimum security requirements for PHI that "a covered entity receives, creates, maintains or transmits in electronic form (ePHI)."[215] Under the Security Rule, covered entities and their business associates must maintain

---

[202] *See* US DEP'T OF HEALTH AND HUMAN SERVICES, *Enforcement Highlights*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (last updated Sep. 30, 2016).
[203] *Id.* Of the remaining cases, 11,099 investigations found that no violation had occurred, and 86,515 cases resulted in a determination that the complaint did not present an eligible case for enforcement.
[204] US DEP'T OF HEALTH AND HUMAN SERVICES, *Enforcement Results by Year*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html.
[205] US DEP'T OF HEALTH AND HUMAN SERVICES, *How OCR Enforces the HIPAA Privacy & Security Rules*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html.
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Summary of the HIPAA Privacy Rule*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/; US DEP'T OF HEALTH AND HUMAN SERVICES, *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/.
[211] *Enforcement Results by Year*, *supra* note 206.
[212] *Id.*
[213] US DEP'T OF HEALTH AND HUMAN SERVICES, *HIPAA Privacy, Security, and Breach Notification Audit Program*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/#program.
[214] *Id.*
[215] *See* SWIRE AND AHMAD, U.S. PRIVATE SECTOR PRIVACY, *supra* note 1, at 49.

the "confidentiality, integrity, and availability of all ePHI the covered entity creates, receives, maintains, or transmits"; protect against reasonable threats or hazards; protect against use or disclosure of ePHI not permitted under the Privacy Rule; and make sure the organization's workforce complies with the Security Rule.[216] The Security Rule also allows organizations to comply by means appropriate to the organization, accounting for factors like size, complexity, costs, technical infrastructure, and the probability and criticality of potential risks to ePHI.[217] Lastly, the Security Rule requires that covered entities conduct ongoing risk assessments, implement security awareness and training for its workforce, and designate an individual responsible for implementing and overseeing the entity's Security Rule compliance program.[218]

[69] Examples of recent OCR enforcement actions include:

1. ***Cignet Health of Prince George's County, Maryland*:** OCR issued a Notice of Final Determination finding that Cignet violated the HIPAA Privacy Rule, imposing a civil money penalty of $4,300,000 USD.[219] OCR found that Cignet had violated 41 patients' rights by denying them access to their medical records.[220] OCR fined Cignet $1,300,000 USD for the violations, and an additional $3,000,000 USD for willful neglect in failing to cooperate with OCR's investigation.[221]

2. ***Massachusetts General Hospital*:** OCR entered into a settlement with Massachusetts General Hospital related to an investigation of the loss of protected health information of 192 patients of its Infectious Disease Associates outpatient practice, including patients with HIV/AIDS.[222] The documents were lost when an employee left them on a subway train while commuting to work.[223] The settlement required Massachusetts General Hospital to pay $1,000,000 USD and enact a robust compliance program to avoid future compliance issues.[224]

3. ***Advocate Health Care Network*:** OCR entered into a settlement with Advocate Health Care Network following an investigation of three reported breaches of ePHI. OCR alleged that Advocate failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities of its ePHI, failed to implement proper policies and procedures to limit access to ePHI, failed to

---

[216] *Id.* at 50-51.
[217] *Id.*
[218] *Id.* at 51.
[219] *See Cignet Health fined a $4.3M Civil Money Penalty for HIPAA Privacy Rule Violations*, US DEP'T OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cignet-health/.
[220] *Id.*
[221] *Id.*
[222] *Massachusetts General Hospital Settles Potential HIPAA Violations*, US DEP'T OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/massachusetts-general-hospital/index.html.
[223] *Id.*
[224] *Id.*

obtain satisfactory assurances that a business associate would properly handle all ePHI in its possession, and failed to reasonably safeguard an unencrypted laptop.[225] The settlement required Advocate to pay $5,550,000 USD and adopt a corrective action plan to address its privacy and security shortcomings.[226]

4. ***University of Mississippi Medical Center (UMMC)*:** OCR entered into a settlement with UMMC related to multiple alleged violations of HIPAA security and privacy requirements, resulting in a penalty of $2,750,000 USD.[227] OCR's investigation alleged that UMMC failed to prevent, detect, contain, and correct security violations; failed to implement physical safeguards for workstations with access to ePHI; failed to assign a unique user name and/or number for identifying and tracking individuals on systems containing ePHI; and failed to notify each individual whose unsecured ePHI was reasonably believed to be at risk as a result of the breach.[228] In addition to the fine, UMMC was required to adopt a corrective action plan to ensure future compliance with HIPAA privacy and safeguard rules.[229]

5. ***Oregon Health & Science University (OHSU)*:** OCR entered into a settlement agreement with OHSU resulting in a comprehensive three-year corrective action plan and a penalty of $2,700,000 USD.[230] OCR investigation began after OHSU submitted multiple breach reports, including two reports involving unencrypted devices and a stolen unencrypted storage device.[231] OCR found that the risk analyses that OHSU conducted did not properly cover all ePHI in OHSU's operation as required.[232] OCR further alleged that OHSU did not act in a timely manner to implement measures to address documented risks and vulnerabilities, nor did it have proper policies and procedures to prevent, detect, contain, and correct security violations.[233] Lastly, OCR alleged that OHSU failed to implement a mechanism to encrypt and decrypt ePHI, or a functional alternative measure, despite knowing that lack of encryption was a risk.[234]

---

[225] *Id.*
[226] *Id.*
[227] *Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC)*, US DEP'T OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/UMMC/index.html.
[228] *Id.*
[229] *Id.*
[230] Press Release, US Dep't of Health and Human Services, Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University (Jul. 18, 2016), http://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html.
[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] *Id.*

IV. Enforcement under US State Law and Private Rights of Action

[70] Section IV introduces privacy enforcement under state law and federal or state private rights of action. Each state has an Attorney General tasked with protecting consumers. As documented by Professor Citron, these AGs have emerged as important privacy enforcers. This Section then examines the numerous private rights of action that exist under both federal and state law, using the state of California as one example. The prevalence of plaintiffs' lawyers and private rights of action in the US means that defendants (including companies and often government agencies) have increased incentive to comply strictly with applicable law.

A. State Attorney General (AG) Enforcement

[71] I next describe an important but sometimes overlooked set of actors in privacy enforcement in the US – the state AGs. The AG in each state serves as the chief law enforcement officer for that state, with a wide range of powers and responsibilities. Professor Danielle Citron of the University of Maryland Law School has recently completed award-winning research about the role of these AGs in US privacy policy and privacy enforcement.[235]

[72] To avoid the complexity of discussing fifty states, my comments here focus on the office of the California AG, which has been a leader in the enforcement of privacy and security related issues.[236] Other state AGs have often taken the lead on specific privacy related issues; my comments here explain the workings in one large state. As Professor Citron's research shows, similar authorities and interest in privacy enforcement exist in other states as well.

[73] California is the most populous state in the US, encompassing approximately 40 million people.[237] Its laws regulating data security broadly encompass any person or business that conducts business in California.[238] Because so much business is online and the population of California is so large, a wide range of businesses headquartered outside of California "conduct business" there and are subject to its data breach and other laws. The impact of enforcement by the California AG is increasing because of the growing use of multi-state collaborations among state AGs, including for large-scale enforcement actions across the country.[239]

[74] A well-known instance of California as a privacy innovator is its passage of the first US state data breach notification law in 2002.[240] Today, at least 46 states and territories have data

---

[235] Citron, *supra* note 4 (manuscript at 9).This research received the best paper award in the 2016 Privacy Law Scholars Conference.

[236] KAMALA D. HARRIS, ATTORNEY GENERAL CALIFORNIA DEPARTMENT OF JUSTICE, CALIFORNIA DATA BREACH REPORT (2016) ("California was the first to enact a data breach notification law, which took effect in 2003. In the twelve years since then, 46 other states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, as well as foreign jurisdictions around the world, have enacted similar laws."), https://oag.ca.gov/breachreport2016.

[237] UNITED STATES CENSUS BUREAU, *California QuickFacts*, http://www.census.gov/quickfacts/table/PST045215/06.

[238] HARRIS, *supra* note 238. The statute also applies to any state or local agency that owns or licenses "computerized data." *Id.*

[239] *Id.*

[240] CAL. CIV. CODE §§ 1798.29, 1798.80 *et seq.*

breach laws, with many of them modeled on the California law.[241] California similarly played the innovator role in other areas, such as when California's laws on restrictive use of consumer data for marketing purposes preceded similar regulations eventually adopted by the FCC.[242] As another example, California was an innovator in credit reporting as the first state to pass credit "freeze" legislation that allows a consumer to lock their credit report, prohibiting access by new credit issuers.[243] These regulations were eventually incorporated into federal law as well.[244]

[75] Enforcement by AGs in California and other US states provides individuals an accessible opportunity for redress for privacy-related violations, within the consumer's own state. The AG solicits complaints from individuals regarding consumer privacy-related violations. Form complaints can be filed by individuals on AG websites, which are accessible to anyone.[245] The AG is permitted to investigate petitions from any persons, including EU data subjects. Once the AG has received complaints relating to a breach of security or other privacy-related violation, the AG may launch an investigation, using a range of investigative tools, such as Civil Investigative Demands requiring companies to turn over information based "merely on suspicion that the law is being violated, or even just because [they] want assurance that it is not."[246]

[76] AG investigations have led to increasingly strict state enforcement of privacy laws. In roughly the past year, investigations by the California AG have resulted in significant settlements with corporate entities for violations of privacy-related laws.[247] For instance, Wells Fargo agreed to an $8.5 million settlement for violating California privacy laws by recording consumers' phone

---

[241] *See* NATIONAL CONFERENCE OF STATE LEGISLATURES, *Security Breach Notification Laws* (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (listing all current state data breach notification laws).

[242] *See, e.g.*, Chris Hoofnagle, European Commission Directorate General Justice, Freedom and Democracy, *Commission Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, B.1 – United States of America*, at 15 (May 2010), http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b1_usa.pdf ("Long before the Federal Communications Commission adopted opt in rules for sharing of telephone subscriber information, the California Public Utilities Code required written consent for transfer of such information.").

[243] *Id.* All fifty states in the U.S. have some form of credit freeze legislation, with 24 states allowing any consumer to place a "freeze" on their credit report. *See, e.g.*, ALA. CODE § 8-35-1 *et seq.*, CAL. CIVIL CODE § 1785.11.2 *et seq.*, KY. REV. STAT. ANN. § 367.363 *et seq.* Others may require a person be a victim of identity theft or a resident of the state. *See, e.g.*, MISS. CODE ANN. § 75-24-201 *et seq.* (allowing credit freezes for victims of identity theft), WASH. REV. CODE § 19.182.170 *et seq.* (allowing credit freezes for any consumer who is a resident of the state). Some also specifically allow for credit freezes on behalf of a "protected consumer" who is either below a certain age or otherwise in guardianship. *See, e.g.*, 815 ILL. COMP. STAT., §505/2MM (allowing a representative on behalf of a disabled person or the guardian of a minor to request a credit freeze on behalf of the minor or disabled person), IND. CODE §§24-5-24-1 *et seq.*, 24-5-24.5-10 *et seq.* (allowing a representative of a "protected consumer" to request a credit freeze on behalf of that protected consumer).

[244] *Id.*, Duties of Card Issuers Regarding Changes of Address, 16 C.F.R. § 681.2(c).

[245] *See, e.g.*, STATE OF CALIFORNIA OFFICE OF THE ATTORNEY GENERAL, *Consumer Complaint Against a Business/Company*, https://oag.ca.gov/contact/consumer-complaint-against-business-or-company (soliciting complaints); *see also* NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL, *New York State Security Breach Reporting Form*, https://forms.ag.ny.gov/CIS/breach-reporting.jsp.

[246] *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950), https://supreme.justia.com/cases/federal/us/338/632/case.html.

[247] *See* STATE OF CALIFORNIA OFFICE OF THE ATTORNEY GENERAL, *Privacy Enforcement Actions*, https://oag.ca.gov/privacy/privacy-enforcement-actions.

calls without a timely disclosure to consumers, as required by the California Penal Code.[248] Comcast resolved an investigation into allegations that it posted consumer information on-line by agreeing to strengthen its restrictions on use of consumer information and paid $25 million in penalties and $8 million to its consumers for restitution.[249] Similarly, Houzz, an online platform for home remodeling that violated California privacy laws through unauthorized recording of telephone calls, appointed a Chief Privacy Officer to oversee its compliance with California and federal privacy laws and paid a fine of $175,000. Warnings to corporate entities by the AG of an impending investigation often serve to facilitate the redress of corporate wrong-doing related to consumer privacy.[250]

[77] If initial investigations do not lead to resolution of a problem, the AG has full power to enforce the laws of the state and the nation on behalf of its constituents.[251] Notably, all fifty states have what are often called "baby FTC Acts." Above, I described the power of the FTC to enforce against deceptive and unfair acts in commerce. California and the other states have "unfair and deceptive acts and practices" (UDAP) laws, with essentially the same enforcement powers as the FTC if a company breaks its privacy promises or acts in an unfair manner toward consumers.

B. Private Rights of Action

[78] It is something of a cliché (and often a true observation) that the US favors plaintiffs more than most other countries. During negotiation of the Safe Harbor in 1999-2000, I heard US Ambassador David Aaron, the lead US negotiator, say more than once to EU negotiators: "We'll take your privacy laws if you take our plaintiffs' lawyers." The prevalence of plaintiffs' lawyers and private rights of action means that defendants (including companies and often government agencies) have increased incentive to comply strictly with applicable law. In the US, the written law is usually not aspirational – it is the basis for enforcement and litigation.

[79] For the many private rights of action under federal and state law, I highlight four ways that US law favors the bringing of such actions:

1. ***Attorney's fees.*** The "American rule" for attorney's fees is that each party generally pays its own lawyers and court expenses. By contrast, the "British rule" is generally that the loser pays the costs of the winning party. This

---

[248] *Id.*
[249] *Id.*
[250] *See, e.g., Massachusetts Attorney General Reaches Settlement with Boston Hospital Over Data Security Allegations*, HUNTON & WILLIAMS PRIVACY & INFORMATION SECURITY LAW BLOG (Nov. 25, 2014), https://www.huntonprivacyblog.com/2014/11/25/massachusetts-attorney-general-reaches-settlement-boston-hospital-data-security-allegations/; FLORIDA OFFICE OF THE ATTORNEY GENERAL, *Attorneys General Reach Settlement with Zappos over Data Breach*, (Jan. 7, 2015), http://www.myfloridalegal.com/newsrel.nsf/newsreleases/F12E26235A23E57785257DC60063AEE9; NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL, *A.G. Schneiderman Announces Settlement with Trump Hotel Collection after Data Breaches Expose over 70K Credit Card Numbers*, (Sep. 23, 2016), http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-trump-hotel-collection-after-data-breaches-expose.
[251] *See* STATE ATTORNEYS GENERAL: POWERS AND RESPONSIBILITIES 14 (Emily Myers, Nat'l Ass'n of Attorneys General eds., 3d ed. 2013).

American rule clearly makes it easier for non-wealthy individuals to pursue a lawsuit.

2. ***Contingency fees.*** The US legal system often features plaintiff lawyers working on contingency fees. A common practice, for instance, is that the attorney will receive one-third or more of any settlement or judgment in a case. The combination of the American rule and contingency fees has created the phenomenon of plaintiff-side law firms that can take a portfolio of cases on contingency. If even a few of the cases succeed, then the law firm can succeed financially.

3. ***Jury trial.*** The right to jury trial, protected in the Seventh Amendment of the US Constitution,[252] remains an important feature of American law. Plaintiffs' lawyers, in my experience, often prefer to have a jury decide a case and the amount of damages rather than the judge. Where juries are outraged by a defendant's behavior, judgments can become quite large and may include punitive damages.

4. ***Broad discovery.*** A fourth feature of US law is relatively broad pre-trial discovery of evidence from the other parties. Although defendants may complain that discovery requests are "fishing expeditions," plaintiffs often can begin a case with a relatively small number of supporting facts, and develop considerably more evidence in the course of discovery.

The combined pro-plaintiff effect of these four factors is substantial compared to a regime that differs on all or most of the factors.

[80] With this pro-plaintiff litigation system in mind, I turn to private rights of action in California as an example of the sorts of laws that also exist in other states. As an initial matter, the California Constitution provides an inalienable right to pursue and obtain privacy.[253] The Privacy Clause "[p]rotects against the unwarranted, compelled disclosure of various private or sensitive information regarding one's personal life, including his or her financial affairs, political affiliations, medical history, sexual relationships, and confidential personnel information."[254]

---

[252] U.S. CONST. amend. VII. ("In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise re-examined in any Court of the United States, than according to the rules of the common law.").

[253] The text provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. Art. 1 § 1; California's Constitution is similar to some other state constitutional provisions protecting privacy. *See, e.g.*, ALASKA CONST. Art. I § 22 ("The right of the people to privacy is recognized and shall not be infringed."); *see also* FLA. CONST. Art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."); *see also* MONT. CONST. Art. 2, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.").

[254] *Tien v. Superior Court*, 139 Cal. App. 4th 528, 539 (Cal. Ct. App. 2006).

Violations of the Privacy Clause are actionable as torts among private actors.[255] California common law has incorporated four privacy torts under which an aggrieved party may sue: (1) intrusion into private matters; (2) public disclosure of private facts; (3) publicity placing a person in a false light; and (4) misappropriation of a person's name or likeness.[256] Depending on the facts alleged for an invasion of privacy, a plaintiff may also include causes of action for fraud and negligence.[257]

[81] In addition to the common law acting under this constitutional guarantee, California has enacted multiple statutes under which aggrieved individuals may seek redress.[258] The following statutes provide a private right of action under California law against any person or business that conducts business in California, and any state or local agency that owns or licenses computerized data.[259]

1. ***California Unfair Competition Law*** (UCL) is the state's "Baby FTC Act" that targets deceptive and unfair behavior. It is a broad and generally-worded statute that protects consumers and businesses from unfair competition described in Section 17200 as: "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising" among other defined acts relating to deceptive practices.[260] The broad coverage of UCL applies to all non-government entities so long as a plaintiff has suffered actual damages as a result of an entity's actions.[261] The UCL provides for injunctive relief, restitution and civil penalties. Injunctive relief and restitution are available in both private-party and government actions.[262] Civil penalties may be imposed in government enforcement actions for violations under UCL but are not available for private actions.[263]

2. ***Confidentiality of Medical Information Act*** (CMIA) protects the confidentiality of individually identifiable medical information obtained from a patient by a health care provider.[264] The CMIA provides that "[n]o provider

[255] *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633 (Cal. 1994), https://scholar.google.com/scholar_case?case=9304848346192844 22&hl=en&as_sdt=6&as_vis=1&oi=scholar.
[256] *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1965) (commonly cited as common law for all fifty states).
[257] *See, e.g.*, *In re EasySaver Rewards Litig.*, 921 F.Supp.2d 1040 (S.D. Cal. 2013), https://casetext.com/case/in-re-easysaver-rewards-litig; *In re Consumer Priv. Cases*, 175 Cal. App. 4th 545, (Cal. Ct. App. 2009), http://www.leagle.com/decision/In%20CACO%2020090701035/CONSUMER%20PRIVACY%20CASES.
[258] California is just an example of one of multiple states that have a robust regulatory scheme for privacy related violations. *See, e.g.*, MASS. GEN. LAWS ch. 214, § 1B, entitled The Massachusetts Privacy Act ("A person shall have a right against unreasonable, substantial or serious interference with his privacy.").
[259] HARRIS, *supra* note 221.
[260] CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*
[261] *See Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 811 (N.D. Cal. 2011) (holding that plaintiffs sufficiently alleged a loss of money or property based on potential unpaid compensation where Facebook used plaintiffs' Facebook profiles to endorse third-party products and services).
[262] *See* CAL. BUS. & PROF. CODE § 17203.
[263] *See id.* § 17206.
[264] The CMIA safeguards much of the same information protected by federal law under HIPAA, but unlike HIPAA, the CMIA creates a private right of action for those affected by a breach of the Act.

of health care, health care service plan, or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c)."[265] Remedies for breach of the CMIA include nominal damages of $1,000 and/or actual damages from "any person or entity who has negligently released confidential information or records."[266]

3. ***California Invasion of Privacy Act*** (CalCIPA) regulates telephone call monitoring and prohibits the intentional recording or eavesdropping of telephone calls without the consent of all parties.[267] A plaintiff may bring an action under CalCIPA so long as one of the parties on the telephone call is located in California. CalCIPA imposes both criminal and civil liability for violators of the statute. For private causes of action, the plaintiff need not suffer actual damages as the statute establishes a $5,000 penalty for each CalCIPA violation.[268] These penalties can quickly accrue as companies who may record or monitor hundreds, if not thousands, of calls each week could be potentially liable for millions of dollars in penalties.[269]

4. ***California Spam Laws*** regulate unsolicited commercial email with misleading or falsified headers or information.[270] They apply to emails sent to or from a California email address and authorize a recipient, an email service provider, or the AG to bring an action for actual damages and liquidated damages of $1,000 per email ad sent in violation, up to one million dollars per incident. They also authorize attorney's fees and costs to a prevailing plaintiff.

5. ***Consumers Legal Remedies Act*** (CLRA) declares unlawful several "methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer."[271] For instance, a plaintiff may rely on the

---

[265] CAL. CIV. CODE § 56 *et seq.*
[266] *Id*. § 56.36(b).
[267] CAL. PENAL CODE § 632(a) makes it unlawful for any person to intentionally eavesdrop upon or record a confidential communication without consent of all parties, whether the communication is in person or by telephone, but excluding cellular or cordless phones; CAL. PENAL CODE § 632.7 makes it unlawful for any person to intercept, receive, or intentionally record a communication without the consent of all parties, and applies where at least one party uses a cellular or cordless phone. This Section has been construed as not requiring that the recorded communications be confidential.
[268] *Id*.
[269] *See, e.g.*, *Young v. Hilton Worldwide*, 565 Fed. App'x 595 (9th Cir. 2014), http://cdn.ca9.uscourts.gov/datastore/memoranda/2014/03/20/12-56189.pdf.
[270] CAL. BUS. & PROF. CODE §§ 17529, 17538.45, http://leginfo.legislature.ca.gov/faces/codes.xhtml.
[271] CAL. CIV. CODE §§ 1750 *et seq.*; *see, e.g.*, NEB. REV. STAT. § 87-302(14) (prohibiting knowingly making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public.), http://nebraskalegislature.gov/laws/statutes.php?statute=87-302; 18 PA. CONS. STAT. § 4107(a)(10) (Pennsylvania's deceptive or fraudulent business practices statute prohibits false and misleading statements in privacy policies published on the Internet), https://govt.westlaw.com/pac/index.

CLRA for misrepresentations for purported tracking of Internet activity.[272] The CLRA allows consumers who suffer damage as a result of a practice declared unlawful to obtain actual damages, an order enjoining the methods, acts, or practices, restitution of property, punitive damages, court costs and attorney's fees, and any other relief that the court deems proper.[273]

[82] In addition to the California statutes that provide a private right of action for corporate actors' wrongdoing, the broad language of the Unfair Competition Law effectively allows private enforcement of a more fulsome regulatory scheme where a plaintiff has suffered damages as a result of "unlawful" actions.[274] California statutes that may be enforced through a private plaintiff's action under a UCL claim include:

1. ***The California Electronic Communications Privacy Act*** (CalECPA) requires government entities to obtain a search warrant before accessing data on an electronic device or from an online service provider.[275]

2. ***The Computer Misuse and Abuse*** law makes it a crime to knowingly access and, without permission, use, misuse, abuse, damage, contaminate, disrupt or destroy a computer, computer system, computer network, computer service, computer data or computer program.[276]

3. ***The California Data Protection Statute*** mandates that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[277] It requires a company to notify affected individuals of a data breach "in the most expedient time possible and without unreasonable delay."[278]

4. ***The Financial Information Privacy Act*** prohibits financial institutions from sharing or selling personally identifiable nonpublic information without obtaining a consumer's consent, as provided.[279] The law requires that (1) a consumer "opt in" before a financial institution may share personal information with an unaffiliated third party, (2) consumers be given an opportunity to "opt

---

[272] *Lane v. Facebook, Inc.*, No. C 08-2010 3845 RS (N.D. Cal., Mar. 17, 2010).
[273] CAL. CIV. CODE § 1780.
[274] *See* CAL. BUS. & PROF. CODE § 17200.
[275] CAL. PENAL CODE § 1546 *et seq.*
[276] *Id.* § 502.
[277] Similarly, Nevada and Minnesota require Internet Service Providers (ISPs) to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Both states prohibit disclosure of personally identifying information, but Minnesota also requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited. MINN. STAT. §§ 325M.01-.09; NEV. REV. STAT. § 205.498.
[278] CAL. CIVIL CODE §§ 1798.29, 1798.82; *see also* Suevon Lee, *Sprouts' W2 Leak In Data-Phishing Scam Prompts Suit*, LAW360 (Apr. 21, 2016), http://www.law360.com/articles/787592.
[279] CAL. FIN. CODE §§ 4050 – 4060.

out" of sharing with a financial institution's financial marketing partners, and (3) consumers be given the opportunity to "opt out" of sharing with a financial institution's affiliates, with some exceptions.

5. ***The Online Privacy Protection Act of 2003*** (CalOPPA) requires operators of commercial web sites or online services that collect personal information on California consumers through a web site to conspicuously post a privacy policy on the site and to comply with its policy.[280] The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information.[281] The privacy policy must also provide information on the operator's online tracking practices. An operator is in violation for failure to post a policy within 30 days of being notified of noncompliance, or if the operator either knowingly and willfully or negligently and materially fails to comply with the provisions of its policy.

[83] California has had a consistently growing set of legal rules providing remedies for violations of privacy and data security. For the reasons discussed at the start of this section, these many private rights of action are more likely to be pursued due to the combination of the American rule for attorney's fees, the prevalence of contingency fees, the use of jury trial, and the availability of broad discovery.

C. Privacy-related Litigation Results in Large Class Action Settlements

[84] There is an important additional reason that US law favors plaintiffs – the use of class actions. Under Rule 23 of the Federal Rules of Civil Procedure, class actions are often available where there are "questions of law or fact common to the class" and "the claims or defenses of the representative parties are typical of the claims or defenses of the class."[282] Applied to privacy and security cases, it is easy to see how a class action can arise – there is one data breach or unlawful privacy practice that applies to numerous consumers. The single violation can lead to issues of law and fact common to the class, and a class can be certified.

[85] My review shows that settlements alone have resulted in approximately $425 million in payments to plaintiffs and government enforcement agencies nationwide over the last ten years.[283] A table at the end of this Chapter lists the major cases. A few examples of cases that yielded multi-million dollar settlements for private plaintiffs in various states include:

1. ***In re Trans Union Corp. Privacy Litigation***, filed in Illinois, resulted in a $75 million settlement where a class of aggrieved plaintiffs alleged that a consumer

[280] CAL. BUS. & PROF. CODE §§ 22575-22579, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=.
[281] Connecticut and Delaware have implemented similar regulation. *See* CONN. GEN. STAT. § 42-471; *see also* DEL. CODE ANN. tit. 6, § 1205C.
[282] FED. R. CIV. P. 23.
[283] *See* Annex 1: Class Action Settlements 2006-2016 at 36.

reporting agency violated the Fair Credit Reporting Act and common law invasion of privacy torts by using consumer information to generate unauthorized target marketing lists.[284]

2. ***Kehoe v. Fidelity Federal Bank and Trust***, filed in Florida, yielded a $50 million settlement for a class of plaintiffs alleging that defendant bank violated the Drivers Privacy Protection Act (DPPA) by purchasing driver information for use in direct marketing.[285]

3. ***Snow v. LensCrafters, Inc.***, filed in California, resulted in a $20 million settlement for a class of plaintiffs alleging that LensCrafters mishandled and misused patients' medical and prescription information in violation of the CMIA and other consumer protection laws.[286]

4. ***In re: WebLoyalty.com, Inc., Marketing and Sales Practices Litigation***, filed in Maryland, resulted in a settlement of $10 million to a class of Plaintiffs alleging that Webloyalty secretly enrolled consumers in a sham discount program as a result of information they provided on various websites in violation of Electronic Funds Transfer Act (EFTA) and ECPA.[287]

[86] In large-scale litigation, plaintiffs serve a functionally similar role as the US government in enforcing consumer protection laws and regulating industries.[288] Private litigation – and the threat of it – continues to lead to more effective compliance by organizations to protect consumers' privacy.

V. Standing to Sue after *Clapper*

[87] The Irish Data Protection Commissioner (DPC) has filed an Affidavit which states that "the 'standing' admissibility requirements of the US federal courts operate as a constraint on all forms of relief available" in the US.[289] This statement appears to refer to the discussion of the US

---

[284] *In re Trans Union Corp. Priv. Litig.*, No. 13-1613 (7th Cir. Jan. 23, 2014), http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2014/D01-23/C:13-1613:J:Hamilton:aut:T:fnOp:N:1278615:S:0 (holding that Trans Union did not violate $75 million settlement when it used those funds to resolve claims arising after the settlement was finalized).

[285] *Kehoe v. Fidelity Federal Bank and Trust*, No. 03-80593-CIV (S.D. Fla. August 1, 2006); *see* K.C. Jones, *Bank to Pay $50 Million for Buying Personal Data*, INFORMATIONWEEK (Aug. 29, 2006), http://www.informationweek.com/bank-to-pay-$50-million-for-buying-personal-data/d/d-id/1046571.

[286] *Snow v. LensCrafters, Inc.*, CGC-02-405544 (Cal. App. Dep't Super. Ct. July 11, 2008); *see* Pete Brush, *LensCrafters Settles $20 Million Indemnification Battle*, LAW360 (Mar. 31, 2009), http://www.law360.com/articles/94630/lenscrafters-settles-20m-indemnification-battle.

[287] *In Re: Webloyalty.com, Inc., Marketing and Sales Practices Litigation*, No. 1:07-MD-018-JLT (D. Mass. Jan. 28, 2009); *see* Julie Zeveloff, *Webloyalty To Pay Back $10M In Fees In MDL Deal*, LAW360 (Feb. 24, 2009), http://www.law360.com/articles/88713/webloyalty-to-pay-back-10m-in-fees-in-mdl-deal.

[288] *See* W. Olson, *Regulation through Litigation*, POINTOFLAW (Aug. 30, 2005) http://www.pointoflaw.com/regulation/overview.php.

[289] *See* Affidavit of John V. O'Dwyer, *Data Protection Comm'r v. Facebook Ireland Ltd*, No. 2016/4809P, para. 93 (filed July 4, 2016) (H.C.).

Supreme Court case *Clapper v. Amnesty International USA* in the DPC's Draft Decision.[290] In *Clapper*, Amnesty International and other plaintiffs brought a constitutional challenge to Section 702 of FISA on the day after it entered into force in 2008.[291] The Supreme Court dismissed the challenge because it found the plaintiffs did not show an injury that granted them standing to sue.

[88] It would be a mistake to read more into *Clapper* than it actually holds. In one sense, I agree with the quotation from the DPC, in the sense that a plaintiff does have to establish standing to sue in order to get relief from a US court. The case should not, however, be read to create a *per se* ban on cases involving US foreign intelligence or counterterrorism programs. Two lower courts, for instance, have found that individuals had standing in the foreign intelligence realm, to challenge the Section 215 telephone metadata program.[292] Another court found, in a counter-terrorism setting, that an individual had standing to challenge suspected placement on the terrorist watch list.[293] The facts and law of the individual case will determine whether an individual has standing to sue.

[89] One concern the Supreme Court identified in *Clapper* is that when US surveillance is challenged in court, affirming or denying an individual's standing to bring the challenge permits him – or an adversary watching the case – "to determine whether he is currently under US surveillance simply by filing a lawsuit."[294] This statement in *Clapper* is consistent with my discussion in Chapter 8, on how hostile actors can seek to use individual remedies to probe an intelligence agency and to learn its national security secrets. Chapter 8 explains in detail how an adversary intelligence agency could deploy an individual remedy to conduct such probes.[295] It also documents how courts in both the EU and US have a clear history of caution about disclosing national security secrets in open court.[296]

[90] Nor has *Clapper* turned out to prevent individuals from bringing lawsuits against companies that commit privacy violations, even in the absence of out-of-pocket damages. Since *Clapper* was decided in 2013, US courts have accepted major class-action litigation against companies such as Adobe Systems[297] and Sony[298] following data breaches. In a number of these cases, courts have affirmed individuals' standing on allegations that data was obtained by unauthorized third parties, without requiring individuals to show any financial or other loss.[299]

---

[290] *See* Draft Decision of the Data Protection Comm'r, *Schrems v. Facebook Ireland Ltd*, No. 3/15/766, para. 55 (May 24, 2016).
[291] *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).
[292] *See, e.g., Am. C.L. Union v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (finding that standing existed to challenge the Section 215 metadata program); *Klayman v. Obama*, 142 F. Supp. 3d 172, 186 (D.D.C. 2015) (same).
[293] *Shearson v. Holder*, 725 F.3d 588, 593 (6th Cir. 2013) (holding that individual had standing to challenge her suspected placement on the terrorist watch list, even though the court found "it is impossible for [her] to prove that her name remains on that list").
[294] *Clapper*, 131 S. Ct. at 1149 n.4.
[295] *See* Chapter 8, Section I(C).
[296] *See* Chapter 8, Sections II-IV.
[297] *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).
[298] *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014).
[299] *See, e.g., Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 WL 4728027, at *3 (6th Cir. Sept. 12, 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015); *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-08617, 2016 WL 5720370, at *4 (N.D. Ill. Oct. 3, 2016), https://docs.justia.com/cases/federal/district-

[91] In addition, the doctrine of standing addressed in *Clapper* pertains only to the US federal courts, and thus at most impacts judicial remedies. This Chapter has identified multiple ways that individuals can seek to address privacy violations in the US, including: judicial remedies; non-judicial remedies (such as the PCLOB and the free press); administrative agency remedies (such as the FTC and FCC); state Attorneys General; and new remedies provided by the Ombudsman and the Umbrella Agreement. Only federal judicial remedies are affected by even the broadest reading of *Clapper*.

[92] All of the above gives reason for caution in interpreting the implications of *Clapper*. Moreover, the DPC has suggested that her findings on the effects of standing may need to be reassessed in light of the Ombudsman and the Umbrella Agreement.[300] Through the Ombudsman mechanism, EU individuals can now lodge complaints regarding US government collection of data. Ombudsman complaints can be brought regardless of whether individuals can show that personal data has been collected, and without needing to show that harm or other adverse consequences were suffered. Similarly, individuals can exercise access rights under the Umbrella Agreement without having to show harm.

VI. Conclusion

[93] This Chapter has sought to present in an organized and understandable way the US system for individual remedies for privacy violations. Section I described judicial remedies against the US government. Section II described non-judicial remedies against the US government, including through complaints to potentially effective organizations. Section III described how suits against non-governmental entities operate, including suits against service providers who provide more information to the government than is allowed. Section IV filled out the enforcement landscape by explaining the role of state law, private rights of action, and class actions in promoting privacy compliance.

[94] As stated in the introduction to this Chapter, these individual remedies complement the systemic safeguards in the US system. Both individual remedies and systemic safeguards play important roles, as discussed further in my Summary of Testimony.

courts/illinois/ilndce/1:2012cv08617/275913/130; *In re Anthem, Inc. Data Breach Litig*., 162 F. Supp. 3d 953, 995 (N.D. Cal. 2016) (holding that "loss of value of personally identifiable information" following a data breach was an injury sufficient to confer standing); *Moyer v. Michaels Stores, Inc*., No. 14 C 561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014), http://il.findacase.com/research/wfrmDocViewer.aspx/xq/fac.20140714_0001468.NIL.htm/qx.

[300] *See* Plaintiff's Reply to the Defence of the First Named Defendant, *Data Protection Comm'r v. Facebook Ireland Ltd*, No. 2016/4809P (filed Sept. 30, 2016) (H.C.), paras. 6(1) & 6(2). The DPC states that "the Draft Decision also needs to be read in the context of the new [Ombudsman mechanism]," and "may need to be read in light of the signing of the 'Umbrella Agreement.'" The DPC states it "could not have had regard" to the Ombudsman or the Umbrella Agreement in reaching its Draft Decision, because neither mechanism had been "implemented at the date of the adoption of the Draft Decision." *Id.*

Annex 1: US Privacy Remedies and Safeguards: Availability to EU Persons

Protection	Authority	Available to EU persons?
Remedy – Petition to US State Department Ombudsman for privacy violations under Privacy Shield, SCCs, or BCRs.[301]	EU-US Privacy Shield Framework	Yes
Remedy – Independent alternative dispute resolution body for privacy violations by Privacy Shield.[302]	EU-US Privacy Shield Framework	Yes
Remedy – Petition for access, correction, or rectification of data sent to US law enforcement.[303]	Umbrella Agreement	Yes
Remedy – Suit against importing or exporting data controller under Standard Contractual Clauses.[304]	Standard Contractual Clauses	Yes
Remedy – Civil suit against US agency and/or individual who unlawfully shares stored content.[305]	Stored Communications Act	Yes
Remedy - Suit against US federal agency for improper handling of data.[306]	Judicial Redress Act, Privacy Act	Yes
Remedy – Civil suit against individuals who unlawfully intercept communications.[307]	Wiretap Act	Yes

[301] *See* Chapter 7, Section I(A)(1) ("Judicial Redress Act, Privacy Shield, and the Umbrella Agreement").
[302] *See id.*
[303] *See id.*
[304] *See id.*
[305] *See* Chapter 7, Section I(A)(2) ("Electronic Communications Privacy Act – Stored Communications Act").
[306] *See* Chapter 7, Section I(A)(1) ("Judicial Redress Act, Privacy Shield, and the Umbrella Agreement").
[307] *See* Chapter 7, Section I(A)(3) ("ECPA – The Wiretap Act").

Protection	Authority	Available to EU persons?
Remedy – Civil suits against individual government officer for unauthorized surveillance.[308]	Foreign Intelligence Surveillance Act	Yes[309]
Remedy – Criminal charges for unlawful access to stored communications.[310]	Stored Communications Act	An EU or US person can petition the US government to pursue criminal charges under its sovereign authority.
Remedy – Criminal charges for unlawful interception of communications.[311]	Electronic Communications Privacy Act	An EU or US person can petition the US government to pursue criminal charges under its sovereign authority.
Remedy – Criminal charges for unauthorized surveillance or disclosure of unauthorized surveillance.[312]	Foreign Intelligence Surveillance Act	An EU or US person can petition the US government to pursue criminal charges under its sovereign authority.
Remedy – Exclusion of unlawfully obtained electronic evidence in a criminal proceeding.[313]	US Constitution, Fourth Amendment	Yes
Remedy – Access to classified evidence necessary to a fair criminal defense.[314]	Confidential Information Procedures Act	Yes
Remedy – Lodge a complaint or request for further investigation with the Privacy and Civil Liberties Oversight Board.[315]	Privacy and Civil Liberties Oversight Board	Yes

[308] *See* Chapter 7, Section I(A)(4) ("Foreign Intelligence Surveillance Act").
[309] Except for individuals who are a "foreign power" or an "agent of a foreign power." 50 U.S.C. § 1801(a)-(b).
[310] *See* Chapter 7, Section I(B) ("US Criminal Judicial Remedies").
[311] *See id.*
[312] *See id.*
[313] *See id.*
[314] *See id.*
[315] *See* Chapter 7, Section II(A) ("The PCLOB").

Protection	Authority	Available to EU persons?
Remedy – Lodge a complaint or request for further investigation with Congressional Intelligence Committees.[316]	Rules of the House of Representatives, Rules of the Senate	Yes
Remedy – Petition the US free press to investigate and report on alleged privacy harms.[317]	US Constitution, First Amendment	Yes
Remedy – Petition companies to communicate data sharing practices through transparency reports.[318]	USA FREEDOM Act	Yes
Remedy – Petition US non-governmental organizations to address alleged privacy harms.[319]	US Constitution, First Amendment	Yes
Remedy – Civil suit against companies that unlawfully share stored communications data with the US government.[320]	Stored Communications Act	Yes
Remedy – Civil suit against persons or entities that unlawfully intercept, disclose, or use surveillance data.[321]	Wiretap Act	Yes
Remedy – Petition to the Federal Trade Commission to investigate alleged privacy harms.[322]	Federal Trade Commission Act	Yes

[316] *See* Chapter 7, Section II(B) ("Congressional Committees").
[317] *See* Chapter 7, Section II(C) ("Individual Remedies through Public Press and Advocacy")
[318] *See id.*
[319] *See id.*
[320] *See* Chapter 7, Section III(A)(1) ("Stored Communications Act").
[321] *See* Chapter 7, Section III(A)(2) ("Wiretap Act").
[322] *See* Chapter 7, Section III(B)(1) ("The FTC").

Protection	Authority	Available to EU persons?
Remedy – Petition to the Federal Communications Commission to investigate alleged privacy harms.[323]	Telecommunications Act	Yes
Remedy – Petition to the Consumer Financial Protection Bureau to investigate alleged privacy harms.[324]	Dodd-Frank Wall Street Reform and Consumer Protection Act	Yes
Remedy – Petition to the Securities and Exchange Commission to investigate alleged privacy harms.[325]	Securities Act	Yes
Remedy – Petition to the Department of Health and Human Services Office of Civil Rights to investigate alleged privacy harms.[326]	Health Insurance Portability and Accountability Act	Yes
Remedy – Petition to US state Attorneys General to investigate and/or prosecute alleged privacy harms.[327]	Various state laws	Yes
Remedy – Private rights of action against US companies for violations of privacy laws and protections under US state and federal law.[328]	Various state and federal laws.	Any limitations on who may bring a suit are determined according to the statute the suit alleges was violated.
Remedy – Class-action litigation for alleged privacy harms.[329]	Various state and federal laws.	Any limitations on who may bring a suit are determined according to the statute the suit alleges was violated.

[323] *See* Chapter 7, Section III(B)(2) ("The FCC").
[324] *See* Chapter 7, Section III(B)(3) ("The CFPB").
[325] *See* Chapter 7, Section III(B)(4) ("The SEC").
[326] *See* Chapter 7, Section III(B)(5) ("The Department of Health and Human Services").
[327] *See* Chapter 7, Section IV(A) ("State Attorney General ('AG') Enforcement").
[328] *See* Chapter 7, Section IV(B) ("Private Rights of Action").
[329] *See* Chapter 7, Section IV(C) ("Privacy-related Litigation Results in Large Class Action Settlements").

Protection	Authority	Available to EU persons?
Safeguard – Oversight of law enforcement searches by independent judicial officers.[330]	US Constitution, Article III	Yes
Safeguard – Requirement of probable cause for physical and digital law enforcement searches.[331]	US Constitution, Fourth Amendment	Yes
Safeguard – "Probable cause plus" requirement for law enforcement wiretaps and real-time interception.[332]	Wiretap Act	Yes
Remedy – Civil suit against law enforcement officials that perform an unlawful search under the Fourth Amendment.[333]	US Constitution, Fourth Amendment	Yes if in the US at the time of the search
Safeguard – Proof-based legal standard for government access in US non-search situations.[334]	Electronic Communications Privacy Act	Yes
Safeguard – Transparency requirements for searches, including notice requirements.[335]	Electronic Communications Privacy Act	Yes
Safeguard – Lack of data retention requirements for Internet communications.[336]	N/A	Yes
Safeguard – Lack of limits on use of strong encryption by persons and businesses.[337]	N/A	Yes

[330] *See* Chapter 4, Section II(A) ("Oversight of Searches by Independent Judicial Officers").
[331] *See* Chapter 4, Section II(B) ("Probable Cause of a Crime as a Relatively Strict Requirement for Both Physical and Digital Searches").
[332] *See* Chapter 4, Section II(C) ("Even Stricter Requirements for Government Use of Telephone Wiretaps and Other Real-time Interception").
[333] *See* Chapter 4, Section II(D) ("The Exclusionary Rule, Preventing Prosecutors' Use of Evidence that Was Illegally Obtained, and Civil Suits").
[334] *See* Chapter 4, Section II(E) ("Other Legal Standards that are Relatively Strict for Government Access in Many Non-Search Situations, such as the Judge-Supervised 'Reasonable and Articulable Suspicion' Standard under ECPA").
[335] *See* Chapter 4, Section II(F) ("Transparency Requirements, such as Notice to the Service Provider of the Legal Basis for a Request").
[336] *See* Chapter 4, Section II(G) ("Lack of Data Retention Rules for Internet Communications").
[337] *See* Chapter 4, Section II(H) ("Lack of Limits on Use of Strong Encryption").

Protection	Authority	Available to EU persons?
Safeguard – Institutional checks and balances on US government authority.[338]	US Constitution	Yes
Safeguard – Independent judicial review of alleged privacy harms.[339]	US Constitution, Article III	Yes
Safeguard – Constitutional protections of individual rights, including privacy.[340]	US Constitution, Bill of Rights	Yes
Safeguard – Democratic accountability for government officials.[341]	US Constitution	Yes
Safeguard – Surveillance reforms after the Snowden disclosures and Presidential Review Group on Intelligence and Communications Technology Report.[342]	EU-US Privacy Shield, Judicial Redress Act, Umbrella Agreement, others.	Yes
Safeguard – Foreign Intelligence Surveillance Court review and oversight of foreign intelligence surveillance practices.[343]	Foreign Intelligence Surveillance Act	Yes
Safeguard – Removal of authority for bulk collection surveillance practices.[344]	USA FREEDOM Act	Yes
Safeguard – Limits on surveillance practices under Section 702 of the FISA Act.[345]	Foreign Intelligence Surveillance Act, Privacy and Civil Liberties Oversight Board Report on Section 702	Yes

[338] *See* Chapter 3, Section I(A) ("A Time-Tested System of Checks and Balances").
[339] *See* Chapter 3, Section I(B) ("Judicial Independence").
[340] *See* Chapter 3, Section I(C) ("Constitutional Protections of Individual Rights").
[341] *See* Chapter 3, Section I(D) ("Democratic Accountability").
[342] *See* Chapter 3, Section II(C) ("The Reforms after the Snowden Disclosures").
[343] *See* Chapter 3, Section III(A)(1) ("The Structure of the FISC under FISA").
[344] *See* Chapter 3, Section III(B) ("Collection of Documents and Other Tangible Things under Section 215").
[345] *See* Chapter 3, Section III(C)(1) ("The Legal Structure of Section 702").

Protection	Authority	Available to EU persons?
Safeguard – Tasking selector limitations on Upstream collection.[346]	Privacy and Civil Liberties Oversight Board Report on Section 702	Yes
Safeguard – Oversight by executive agency Inspectors General.[347]	Inspector General Act	Yes
Safeguard – Congressional oversight and investigation of foreign intelligence activities.[348]	US Constitution Article II, Rules of the House of Representatives, Rules of the Senate	Yes
Safeguard – Independent review by the Presidential Review Group.[349]	N/A	Yes
Safeguard – Independent oversight and review by the Privacy and Civil Liberties Oversight Board.[350]	9/11 Commission Act	Yes
Safeguard – Office of the Director of National Intelligence oversight of the intelligence community.[351]	US Constitution, Article II	Yes
Safeguard – Federal Privacy Council for US government agencies stewardship and assistance to federal agency privacy professionals.[352]	Executive Order 13,719	Yes
Safeguard – Executive branch transparency about surveillance activities, including declassified FISC opinions.[353]	USA FREEDOM Act	Yes

[346] *See* Chapter 3, Section III(C)(3) ("The Upstream Program").
[347] *See* Chapter 3, Section IV(A) ("Executive Agency Inspectors General").
[348] *See* Chapter 3, Section IV(B) ("Legislative Oversight").
[349] *See* Chapter 2, Section (B)(4) ("President Obama's Review Group on Intelligence and Communications Technology, 2013-14").
[350] *See* Chapter 3, Section IV(C) ("Independent Review: Review Group and PCLOB").
[351] *See* Chapter 3, Section IV(D) ("The Federal Privacy Council and Privacy and Civil Liberties Offices in the Agencies").
[352] *See id.*
[353] *See* Chapter 3, Section V(A) ("Greater Transparency by the Executive Branch about Surveillance Activities").

Protection	Authority	Available to EU persons?
Safeguard – USA FREEDOM Act provisions mandating public law about major FISC decisions.[354]	USA FREEDOM Act	Yes
Safeguard – Transparency reports by the US Government regarding national security investigations.[355]	USA FREEDOM Act	Yes
Safeguard – US intelligence community Statistical Transparency Reports.[356]	USA FREEDOM Act	Yes
Safeguard – Company issued transparency reports on the range of orders they have replied to.[357]	USA FREEDOM Act	Yes
Safeguard – Principle in signals intelligence activities to protect the privacy rights of non-US persons.[358]	Presidential Policy Directive 28	Yes
Safeguard – Protection of civil liberties of foreign persons beyond privacy.[359]	Presidential Policy Directive 28	Yes
Safeguard – Minimization of personal information acquired during signals intelligence activities.[360]	Presidential Policy Directive 28	Yes
Safeguard – Limits on the retention and dissemination of signals intelligence.[361]	Presidential Policy Directive 28	Yes

[354] *See* Chapter 3, Section V(B) ("USA FREEDOM Act Provisions Mandating Public Law about Major FISC Decisions").
[355] *See* Chapter 3, Section V(D) ("Transparency Reports by the US Government").
[356] *See id.*
[357] *See* Chapter 3, Section V(E) ("Transparency Reports by Companies").
[358] *See* Chapter 3, Section VI(B)(1) ("Privacy is Integral to the Planning of Signals Intelligence Activities").
[359] *See* Chapter 3, Section VI(B)(2) ("Protection of Civil Liberties in Addition to Privacy").
[360] *See* Chapter 3, Section VI(B)(3) ("Minimization Safeguards").
[361] *See* Chapter 3, Section IV(B)(4) ("Retention, Dissemination, and Other Safeguards for Non-US Persons Similar to Those for US Persons").

Protection	Authority	Available to EU persons?
Safeguard – Purpose limitations on signals intelligence collected in large quantities without the use of discriminants.[362]	Presidential Policy Directive 28	Yes
Safeguard – Prohibition of the use of signals intelligence to gain a competitive advantage for US companies and the US business sector commercially.[363]	Presidential Policy Directive 28	Yes
Safeguard – Publication of implementation procedures under Presidential Policy Directive 28.[364]	Presidential Policy Directive 28	Yes
Safeguard – Requirement to use selectors and identifiers to focus intelligence collections.[365]	Presidential Policy Directive 28	Yes
Safeguard – White House oversight of foreign intelligence procedures.[366]	Presidential Policy Directive 28	Yes
Safeguard – White House process to disclose software vulnerabilities.[367]	US Constitution, Article II	Yes
Safeguard – Umbrella Agreement data protection framework for data exchanged between the EU and US for law enforcement purposes.[368]	Umbrella Agreement	Yes
Safeguard – Privacy Shield creation of commitments from the US government to	US EU Privacy Shield Framework	Yes

[362] *See* Chapter 3, Section IV(B)(5) ("Limits on Bulk Collection of Signals Intelligence").
[363] *See* Chapter 3, Section IV(B)(6) ("Limits on Surveillance to Gain Trade Secrets for Commercial Advantage").
[364] *See* Chapter 3, Section IV(B)(7) ("Discussion of PPD-28").
[365] *See id.*
[366] *See* Chapter 3, Section IV(C) ("New White House Oversight of Sensitive Intelligence Collection, including of Foreign Leaders").
[367] *See* Chapter 3, Section IV(D) ("New White House Process to Help Fix Software Flaws, rather than Use Them for Surveillance").
[368] *See* Chapter 3, Section IV(F) ("The Umbrella Agreement as a Systemic Safeguard").

Protection	Authority	Available to EU persons?
address EU data protection concerns and work with EU DPAs.[369]		

[369] *See* Chapter 3, Section IV(G) ("Privacy Shield as a Systemic Safeguard").

Annex 2: Class Action Settlements 2006-2016

Total Settlement Amount: $425,005,400

Case	Claims	Settlement Amount	Case Citation
In re Trans Union Corp. Privacy Litigation, No. 1:00-cv-04729 (N.D. Ill. May 30, 2008)	Plaintiffs alleged that consumer reporting agency violated the FCRA by using consumer credit information to generate target marketing lists and by providing those lists to its consumers. Claims included violations of the FCRA, invasion of privacy, misappropriation, violation of the Cal. UCL, and unjust enrichment.	$75,000,000	*In re Trans Union Corp. Priv. Litig.*, No. 13-1613 (7th Cir. Jan. 23, 2014) (holding that Trans Union did not violate $75 million settlement when it used those funds to resolve claims arising after the settlement was finalized), http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2014/D01-23/C:13-1613:J:Hamilton:aut:T:fnOp:N:1278615:S:0.
Kehoe v. Fidelity Federal Bank and Trust, No. 03-80593-CIV (S.D. Fla. Aug. 1, 2006)	Plaintiffs alleged bank violated the DPPA when it purchased 565,000 names and addresses for use in direct marketing.	$50,000,000	K.C. Jones, *Bank to Pay $50 Million for Buying Personal Data*, INFORMATIONWEEK (Aug. 29, 2006, 4:32 PM), http://www.informationweek.com/bank-to-pay-$50-million-for-buying-personal-data/d/d-id/1046571.

Case	**Claims**	**Settlement Amount**	**Case Citation**
United States v. Google, Inc., 3:12-cv-04177-SI (N.D. Cal. Aug. 9, 2012)	FTC alleged that Google violated a consent order by circumventing privacy settings for Apple's Safari browser despite promising to honor them. The FTC claimed violations of the FTCA arising from collecting information covered in the consent order, serving targeted advertisements, and misrepresenting code compliance. Google also settled with the Attorneys General of 37 states.	$39,500,000	Claire Cain Miller, *Google to Pay $17 Million to Settle Privacy Case*, N.Y. TIMES, Nov. 18, 2013, http://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html?_r=0.
In re: EasySaver Rewards Litigation, MDL No. 09-2094 (S.D. Cal. Feb. 4, 2013)	Plaintiffs alleged that Provide Commerce transmitted its consumers' private payment information to third-party marketing partners, who then charged consumer's credit accounts without permission under the guise that the consumer supposedly joined savings programs such as EasySaver Rewards. Plaintiffs claimed violations of the California unfair competition law, the California Consumers Legal Remedies Act, and the Federal Electronics Funds Transfer Act. They also alleged fraud, breach of contract, breach of the implied covenant of good faith and fair dealing, invasion of privacy, unjust enrichment and negligence.	$21,365,000	Megan Leonhardt, *ProFlowers Parent Co. Arranges $38M Deal Over Data Policies*, LAW360 (June 14, 2012, 2:19 PM), http://www.law360.com/articles/350092/proflowers-parent-co-arranges-38m-deal-over-data-policies.

Case	**Claims**	**Settlement Amount**	**Case Citation**
In Re: Department of Veterans Affairs (VA) Data Theft Litigation, MDL No. 1796, Action No. 06-0506 (D.D.C. Sep. 11, 2009), https://www.courtlistener.com/opinion/2667294/in-re-department-of-veterans-affairs-va-data-theft/.	This litigation centered on a stolen external hard drive that contained the personal information of millions of veterans. The plaintiffs claimed that the VA showed a reckless disregard for veterans' privacy rights and an intentional and willful disregard for Privacy Act requirements by failing to interview the employee in question until 12 days after the theft and five days after the VA's inspector general learned of the theft.	$20,000,000	Associated Press, *$20 Million Settlement Reached for Veterans in ID Theft Suit*, N.Y. TIMES, Jan. 27, 2009, http://www.nytimes.com/2009/01/28/washington/28vets.html.
Fraley v. Facebook, Inc., No. 5:11-cv-0176 (N.D. Cal. Aug. 26, 2013)	Plaintiffs alleged that Facebook used members' pictures in ads without their consent.	$20,000,000	Emily Field, *Facebook's $20M Ad Settlement Kosher, 9th Cir. Says*, LAW360 (Jan. 6, 2016, 5:54 PM), http://www.law360.com/articles/743306/facebook-s-20m-ad-settlement-kosher-9th-circ-says.
Snow v. LensCrafters, Inc., CGC-02-405544 (Cal. Sup. Ct. July 11, 2008)	Plaintiffs alleged that the optometrists and LensCrafters mishandled and misused the patients' medical and prescription information in violation of California's CMIA and other consumer protection laws.	$20,000,000	Pete Brush, *LensCrafters Settles $20 Million Indemnification Battle*, LAW360 (Mar. 31, 2009, 12:00 AM), http://www.law360.com/articles/94630/lenscrafters-settles-20m-indemnification-battle.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Marenco v. Visa, Inc., 2:10-cv-08022 (C.D. Cal. Nov. 30, 2011)	Plaintiff alleged Visa recorded thousands of telephone calls to customer service representatives without permission or disclosure. Plaintiff claimed this violated recording laws in several states.	$18,000,000	Bibeka Shrestha, *Visa Hangs Up Call Recording Class Action For $18M*, LAW360 (Oct. 24, 2011, 5:36 PM), http://www.law360.com/articles/280110/visa-hangs-up-call-recording-class-action-for-18m.
Harris v. ComScore Inc., No. 1:11-cv-05807 (N.D. Ill. May 30, 2014)	Plaintiffs alleged that online data analytics company ComScore installed data harvesting software on users' computers without consent, which allowed them to surveil and sell private information. Plaintiffs claimed violations of the SCA, ECPA, and other causes of action.	$14,000,000	Andrew Scurria, *ComScore Pays $14M To Escape Massive Privacy Class Action*, LAW360 (June 4, 2014, 2:54 PM), http://www.law360.com/articles/544569/comscore-pays-14m-to-escape-massive-privacy-class-action
Perkins v. LinkedIn Corp., 5:13-cv-04303 (N.D. Cal. Sep. 15, 2015), https://casetext.com/case/perkins-v-linkedin-corp-2	Plaintiffs asserted that LinkedIn took users' email addresses and used them to harvest additional email addresses from the users' external accounts. They alleged that LinkedIn used the email addresses to send an initial contact and at least two follow-up emails to those in the users' address books, making it look like the email was sent or endorsed by the user, in an effort to acquire more members, especially premium-paying members. Plaintiffs claimed that they did not agree to allow the emails to be sent.	$13,000,000	Seung Lee, *LinkedIn to pay $13 Million in Suit Settlement for Excessively Spamming Users*, NEWSWEEK (Oct. 5, 2015, 2:59 PM), http://www.newsweek.com/linkedin-13-million-class-action-lawsuit-emails-379975.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Reed v. 1-800 Contacts, Inc., MDL No. 12-2359 (S.D. Cal. Jan. 2, 2014)	1-800-Contacts allegedly recorded telephone calls made to and received from California residents without their consent in violation of the CIPA.	$11,700,000	Juan Carlos Rodriguez, *1-800 Contacts Agrees To Pay $11.7M In Call-Recording Suit*, LAW360 (Nov. 19, 2013, 5:01 PM), http://www.law360.com/articles/489934/1-800-contacts-agrees-to-pay-11-7m-in-call-recording-suit.
Utility Consumer's Action Network v. Bank of America, N.A., No. CJC-01-004211 (Cal. App. Dep't Super. Ct. Apr. 12, 2007)	Plaintiffs alleged that the Bank of America disclosed nonpublic, personal information belonging to its customers to third-party marketers in exchange for money, without customers' consent or proper notice. They alleged unlawful, unfair and fraudulent business practices, invasion of privacy and unjust enrichment.	$10,750,000	CENTER FOR JUSTICE AND DEMOCRACY AT N.Y. LAW SCHOOL, CLASS ACTIONS ARE CRITICAL TO REMEDY INVASIONS OF PRIVACY (2014), https://centerjd.org/system/files/ClassActionPrivacyF.pdf.
In Re: Webloyalty.com, Inc., Marketing and Sales Practices Litigation, No. 1:07-MD-018-JLT (D. Mass. Jan. 28, 2009)	Plaintiffs alleged that Webloyalty secretly enrolled consumers in a $7-10/month sham discount program if they filled out a discount pop-up on websites such as Priceline and Fandango. Part of this process included obtaining card information from the retailer without the consumer's consent. The class sought relief under the EFTA, ECPA, and Civil Theft.	$10,000,000	Julie Zeveloff, *Webloyalty To Pay Back $10M In Fees In MDL Deal*, LAW360 (Feb. 24, 2009, 12:00 AM), http://www.law360.com/articles/88713/webloyalty-to-pay-back-10m-in-fees-in-mdl-deal.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Lane v. Facebook, Inc., No. C 08-3845 RS (N.D. Cal. Mar. 17, 2010)	Plaintiffs alleged Facebook transmitted personal information obtained from its Beacon program websites back to the Facebook site without the consent of the user. They claimed violations of ECPA, the Video Privacy Protection Act (VPPA), and state law.	$9,500,000	Juan Carlos Perez, *Facebook Will Shut Down Beacon to Settle Lawsuit*, N.Y. TIMES, Sept. 19, 2009, http://www.nytimes.com/external/idg/2009/09/19/19idg-facebook-will-shut-down-beacon-to-settle-lawsuit-53916.html.
Batmanghelich v. Sirius XM Radio Inc., No. 09-cv-09190 (C.D. Cal. Mar. 7, 2011)	Plaintiffs in five states alleged that Sirius XM was illegally recording phone calls in violation of state privacy statutes.	$9,500,000	Richard Vanderford, *Sirius Settles Privacy Suit With 5 States For $9.5M*, LAW360 (Mar. 11, 2011, 11:13 PM), http://www.law360.com/articles/232199/sirius-settles-privacy-suit-with-5-states-for-9-5m.
In re Carrier iQ Inc. Consumer Privacy Litigation, No. 3:12-md-02330 (N.D. Cal. Jan. 22, 2016)	Plaintiffs alleged that Carrier IQ's software, which was designed to help determine the cause of dropped cell phone calls, was transmitting sensitive information from users' phones. The plaintiffs claimed violations of the Federal Wiretap Act and many state privacy acts and consumer protection laws.	$9,000,000	Joe Van Acker, *Carrier IQ, Samsung Ink $9M Deal To End Privacy Suit*, LAW360 (Jan. 25, 2016, 5:18 PM), http://www.law360.com/articles/750372/carrier-iq-samsung-ink-9m-deal-to-end-privacy-suit.

Case	**Claims**	**Settlement Amount**	**Case Citation**
In re Netflix Privacy Litigation, 5:11-cv--00379 (N.D. Cal. Mar. 18, 2013), http://www.leagle.com/decision/In%20FDCO%2020130319A55/IN%20RE%20NETFLIX%20PRIVACY%20LITIGATION	Plaintiffs alleged that Netflix kept former customers' information long after the users had canceled their accounts. They claimed this practice violated a provision of the VPPA.	$9,000,000	Allison Grande, *Netflix Tells 9th Circ. Its $9M Privacy Deal Passes Muster*, LAW360 (Oct. 31, 2013, 7:56 PM), http://www.law360.com/articles/485252/netflix-tells-9th-circ-its-9m-privacy-deal-passes-muster.
In re Google Buzz Privacy Litigation, 5:10-cv-00672-JW (N.D. Cal. Sep. 3, 2010), https://epic.org/privacy/ftc/googlebuzz/buzz_settlement.pdf	Plaintiffs alleged that Google Buzz, a social networking product, violated their privacy by creating publically-available lists of networking contacts based on an individual's email and chat history. Plaintiffs claimed this practice violated ECPA.	$8,500,000	Ben Parr, *Google Settles Buzz Privacy Lawsuit for $8.5 Million*, MASHABLE (Sept. 3, 2010), http://mashable.com/2010/09/03/google-buzz-lawsuit-settlement/#ePEqKHR5mkqf.
In re Google Referrer Header Privacy Litigation; No. 10-cv-04809 (N.D. Cal. Mar. 31, 2015), https://casetext.com/case/in-re-google-referrer-header-privacy-litig-1	Plaintiffs alleged that Google improperly provided websites with the Google search terms directing a particular user to that website and that the search terms contained personal information. Plaintiffs claimed this violated the SCA.	$8,500,000	*Google Agrees to Pay $8.5 Million to Settle Claims It Disclosed Internet Search Queries*, BLOOMBERG BNA (July 29, 2013), http://www.bna.com/google-agrees-pay-n17179875501/.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Kinder v. Meredith Corp., No. 1:14-cv-11284 (E.D. Mich. Feb. 4, 2016)	Plaintiffs claimed that Meredith Corp. violated Michigan's Video Rental Privacy Act by disclosing subscribers' personal data.	$7,500,000	Allison Grande, *$7.5M Deal In Mich. Magazine Privacy Row Gets Initial Nod*, LAW360 (Feb. 5, 2016, 10:28 PM), http://www.law360.com/articles/755931/7-5m-deal-in-mich-magazine-privacy-row-gets-initial-nod.
Mount v. Wells Fargo Bank, N.A., No. B260585 (Cal. App. Ct. Feb. 9, 2016), http://www.courts.ca.gov/opinions/nonpub/B260585.PDF	Plaintiffs alleged that Wells Fargo secretly recorded customer service phone calls in violation of CalCIPA. The California Court of Appeals affirmed the settlement.	$5,600,000	Joe Van Acker, *Calif. Court Upholds $5.6M Wells Fargo Privacy Settlement*, LAW360 (Feb. 11, 2016, 1:46 PM), http://www.law360.com/articles/758023/calif-court-upholds-5-6m-wells-fargo-privacy-settlement.
Cohorst v. BRE Properties, Inc., No. 3:10-cv-02666 (S.D. Cal. Apr. 29, 2011)	Plaintiffs alleged that BRE properties recorded phone conversations without notice or consent. Their claims included recording laws from 14 states as well as common law invasion of privacy and negligence counts.	$5,500,000	*Cohorst v. BRE Props.*, No. 3:10-CV-2666-JM-BGS, 2011 U.S. Dist. LEXIS 151719 (S.D. Cal. Nov. 9, 2011) (approving $5.5 million settlement for approximately 1,300 people who made calls that were recorded by company without consent).

Case	**Claims**	**Settlement Amount**	**Case Citation**
Coulter-Owens v. Rodale Inc., No. 2:14-cv-12688 (E.D. Mich. May 3, 2016), http://law.justia.com/cases/federal/district-courts/michigan/miedce/2:2014cv12688/292915/44/	Plaintiffs alleged Rodale violated Michigan's Video Rental Privacy Act by disclosing its customers' magazine subscription information and subscription histories to third-party marketing companies without first obtaining the consent of the consumers.	$4,500,000	Anthony Salamone, *Rodale Settles Michigan Lawsuit over Subscriber Privacy for $4.5 Million*, MORNING CALL (June 17, 2016), http://cqrcengage.com/uwmich/app/document/14384322.
Holland v. Yahoo Inc., No. 5:13-cv-04980 (N.D. Cal. Aug. 25, 2016)	Plaintiffs were a class of non-Yahoo users who alleged that Yahoo scanned users' emails before the users had even seen them in an effort to tailor marketing efforts. They claimed this violated CalCIPA.	$4,000,000	Brandon Lowrey, *Yahoo Email Privacy Deal OK'd With $4M In Attys' Fees*, LAW360 (Aug. 26, 2016), http://www.law360.com/articles/833112/yahoo-email-privacy-deal-ok-d-with-4m-in-attys-fees.
In re Quantcast Advertising Cookie Litigation, No. 2:10-cv-05484 (C.D. Cal. Dec. 3, 2010)	Plaintiffs alleged Quantcast and the other websites set up flash cookies on the users' computers to use as local storage within the flash media player to back up browser cookies for purposes of restoring them later. Their claims included violations of the Computer Fraud and Abuse Act, ECPA, the VPPA, and various California state laws.	$2,400,000	Zach Winnick, *ABC, Others Settle Action Over Web Privacy Breaches*, LAW360 (June 13, 2011), http://www.law360.com/articles/251066/abc-others-settle-action-over-web-privacy-breaches.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Curry v. AvMed, Inc., No. 1:10-cv-24513-JLK (S.D. Fla. September 3, 2013)	Plaintiffs brought a breach of contract and privacy class action against a healthcare insurer that had laptops with unencrypted customer information stolen.	$3,000,000	Allison Grande, *AvMed, Customers Reach Settlement In Data Theft Suit*, LAW360 (Sept. 6, 2013, 7:53 PM), http://www.law360.com/articles/470677/avmed-customers-reach-settlement-in-data-theft-suit.
Petersen v. Lowes HIW, Inc., 3:11-cv-01996-RS (N.D. Cal. Aug. 24, 2012)	Plaintiffs alleged that Lowes improperly recorded zip codes and other personal information in order to obtain home addresses for marketing purposes. Plaintiffs claimed this practice violated a California law that prevents a merchant from requesting personal identification information as a condition to accepting credit card payments.	$2,900,000	Brian Mahone, *Lowe's To Pay $3M To Settle ZIP Code Collection Suits*, LAW360 (Apr. 27, 2012, 4:39 PM), http://www.law360.com/articles/334871/lowe-s-to-pay-3m-to-settle-zip-code-collection-suits.
Minnesota v. Accretive Health, Inc., 0:12-cv-00145 (D. Minn. July 30, 2012)	State of Minnesota alleged that a debt collector for two hospital systems violated state privacy laws when a laptop containing patient data was stolen.	$2,490,400	Tony Kennedy & Maura Lerner, *Accretive is Banned from Minnesota*, STAR TRIBUNE, July 21, 2012, http://www.startribune.com/accretive-banned-from-minnesota-for-at-least-2-years-to-pay-2-5m/164313776/.

Case	**Claims**	**Settlement Amount**	**Case Citation**
Fort Hall Landowners Alliance, Inc. v. Department of Interior, No. 4:99-cv-00052-BLW (D. Idaho Dec. 24, 2007)	Group of Native Americans brought suit against the Bureau of Indian Affairs. They claimed the Bureau violated the Privacy Act by disclosing personal information connected to renewals of leases of allotment land.	$2,350,000	Stipulation for Approval of Class Settlement, *Fort Hall Landowners Alliance, Inc. v. Department of Interior*, No. 4:99-cv-00052-BLW, ECF No. 418 (D. Idaho Sept. 19, 2007).
Stone v. Howard Johnson International, Inc., 2:12-cv-01684 (C.D. Cal. Aug. 26, 2015)	Plaintiffs alleged that Howard Johnson and Wyndham hotels were surreptitiously recording customers' phone calls. Plaintiffs claimed violations of California's Privacy Act.	$1,500,000	Linda Chiem, *HoJo, Wyndham Settle Phone Privacy Class Action For $1.5M*, LAW360 (Apr. 27, 2015), http://www.law360.com/articles/648047/hojo-wyndham-settle-phone-privacy-class-action-for-1-5m.
Brown v. Defender Security Company, 2:12-cv-07319 (C.D. Cal. Sept. 12, 2013)	Plaintiffs alleged that a home security company surreptitiously recorded customers' phone calls. Plaintiffs claimed violations of California's Privacy Act.	$1,400,000	Gavin Broady, *Calif. Security Co. Pays $1.4M To Settle Recorded Call Suit*, LAW360 (Sept. 16, 2013, 1:07 PM), http://www.law360.com/articles/472856/calif-security-co-pays-1-4m-to-settle-recorded-call-suit.
In the Matter of Cellco Partnership, d/b/a Verizon Wireless, FCC Rcd DA 16-242 (Mar. 7,	The FCC investigated Verizon to determine whether its "supercookies" that tracked Internet activity broke privacy and data security laws. Verizon settled in order to end the investigation.	$1,300,000	Press Release, FCC, FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-In for Third Parties (Mar. 7, 2016), https://apps.fcc.gov/edocs_publi

Case	Claims	Settlement Amount	Case Citation
2016), https://apps.fcc.gov/edocs_public/attachmatch/DA-16-242A1.pdf			c/attachmatch/DOC-338091A1.pdf.
Saunders v. StubHub, Inc., CGC-12-517707 (Cal. App. Dep't Super. Ct. Apr. 9, 2015)	Plaintiffs alleged that StubHub's customer service line recorded customer's calls without notice or consent. They claimed violations of the California Invasion of Privacy Act.	$1,250,000	Beth Winegarner, *StubHub Gets Nod For Deal After Prior Version Didn't 'Add Up'*, LAW360 (July 14, 2015), http://www.law360.com/articles/679170/stubhub-gets-nod-for-deal-after-prior-version-didn-t-add-up.
United States v. Xanga.com, Inc., No. 06 CV 6853 (S.D.N.Y. Sep. 12, 2006), https://www.ftc.gov/sites/default/files/documents/cases/2006/09/xangaconsentdecree_image.pdf	The FTC alleged that a blog hosting website knowingly collected and distributed personal information of children under 13 in violation of COPPA.	$1,000,000	Press Release, FCC, Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule (Sept. 7, 2006), https://www.ftc.gov/news-events/press-releases/2006/09/xangacom-pay-1-million-violating-childrens-online-privacy.

Case	**Claims**	**Settlement Amount**	**Case Citation**
United States v. Sony BMG Music Entertainment, No. 08 Civ. 10730 (S.D.N.Y. Dec. 15, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211consentp0823071.pdf	The FTC alleged that Sony allowed tens of thousands of children under age 13 to register on its websites and create personal fan pages where they could interact with other Sony Music fans, including adults, despite knowing the age of the children via the personal information they submitted. The FTC claimed this violated COPPA.	$1,000,000	Press Release, FCC, Sony BMG Music Settles Charges Its Music Fan Websites Violated the Children's Online Privacy Protection Act (Dec. 11, 2008), https://www.ftc.gov/news-events/press-releases/2008/12/sony-bmg-music-settles-charges-its-music-fan-websites-violated.

CHAPTER 8:

INDIVIDUAL REMEDIES, HOSTILE ACTORS, AND NATIONAL SECURITY CONSIDERATIONS

[1] This Chapter examines how individual remedies for privacy violations relate to the risk that hostile actors will use remedies to learn national security secrets. Part 2 of the Summary of Testimony discusses a central theme of my testimony, that we need systemic safeguards against excessive surveillance. Notably, systemic safeguards include transparency where feasible and oversight by institutions that have access to top secret information, such as the Foreign Intelligence Surveillance Court (FISC) and the Privacy and Civil Liberties Oversight Board (PCLOB). Part 3 of the Summary of Testimony examines the multiple ways that individuals can achieve remedies in the US for privacy violations. As discussed there, the US in numerous respects has a legal system that favors enforcement and individual remedies, including features such as: use of contingency fees (so a plaintiff does not need to be wealthy); parties pay their own litigation costs (so a losing plaintiff does not pay defendants' costs); jury trials; broad discovery rules; and easier certification of class actions.

[2] The Summary of Testimony also discusses a caveat about individual remedies in the intelligence setting. That caveat is the subject of the current Chapter. The desirability of individual remedies in intelligence systems must be weighed against the risks that come from disclosing classified information. In the terms used in Article 8 of the European Convention on Human Rights, the availability of the individual right to privacy for intelligence systems is assessed against the necessity in a democratic society of the interests of national security and public safety.

[3] The field of cybersecurity provides an analogy for deciding what types of remedies individuals should have about processing of their information by surveillance agencies. The idea I am suggesting is simple but I believe helpful – be cautious about creating a new vector of attack, such as individual remedies, into a protected system such as an intelligence agency.

[4] A simple example illustrates the sort of harm to national security that could result from individuals' direct access to their data held by an intelligence agency. Suppose a hostile actor, such as a foreign intelligence service, wants to probe the NSA or a Member State intelligence agency. The hostile actor may have Alice use a text service, Bob an email service, and Carlos a chat service. Each of them then file access requests, and only Bob has a file. If so, then the hostile actor has learned something valuable – the email service is under surveillance, but the text and chat services appear not to be. In this example, the individual remedy becomes an attack vector, or form of cyberattack – the hostile actor can probe the agency's secrets, and learn its sources and methods.

[5] Section I of this Chapter provides more detailed discussion of how a foreign intelligence agency or other hostile actor could use individual remedies to probe an intelligence agency, as a form of cyberattack. It also points out that attacks against intelligence agencies are not hypothetical – they occur every day by the most capable adversaries in the world. In short, restricted access to an intelligence agency's secrets can be seen predominantly as a security feature, rather than being a privacy bug.

[6] Sections II and III of this Chapter develop an important, related point – both European and US courts have already created doctrines to prevent this sort of attack. In the US, courts in certain instances recognize what is called the "state secrets doctrine," so that judges (while

maintaining overall supervision of a case) take care not to let individual litigation become a route of attack on national security secrets. Similar judicial decisions appear to be the norm in Europe, with judges protecting against disclosure or use of national security information in open proceedings. In other words, established law recognizes limits on individual remedies in the foreign intelligence area.

[7] Section IV of this Chapter discusses the importance of protecting individual rights in criminal cases, while also protecting classified secrets. I describe the US Classified Information Procedures Act (CIPA), which sets forth procedures for a criminal defendant to have access to classified information in a criminal case. Similar to my discussion of systemic safeguards, CIPA provides two important safeguards: (1) supervision by an independent judge; and (2) access by the judge and other participants to classified information, without disclosing classified information publicly.

I. Hostile Actors and the Analogy to Cybersecurity

[8] This Section briefly explains why intelligence agencies are high value targets for attack, including from the intelligence agencies and military operations of hostile actors. It explains the analogy to cybersecurity attacks, and concludes with a discussion of the risks of revealing national security secrets.

A. Intelligence Agencies are High Value Targets for Attack

[9] An intelligence agency such as the US National Security Agency or the German Bundesnachrichtendienst (BND) is a constant target for hostile actors, such as the military and intelligence services of adversary nations.[1] State secrets, including state surveillance secrets, are high value targets for hostile actors. Access by a hostile actor, for instance, could allow the hostile actor to gain access to: the surveillance information collected (including communications of data subjects); the types of services the agency is tracking; the specific targets under investigation; the identity of the agency's intelligence assets; and much more. Hostile actors may be especially interested in counterintelligence information – what does the agency under attack know about the hostile actor's own operations and possible spies within the agency? Suppose, at the extreme, that all of the NSA's and BND's activities were known to adversaries; in such a case, hostile terrorists or nation states would gain a large advantage against the NSA and BND, with in my view serious consequences to national security.

[1] Although any computer system today is subject to cyberattack, national intelligence agencies, with their numerous national security secrets, are subject to incessant attacks from advanced persistent threats. *Worldwide Cyber Threats: Hearing before the H. Permanent Select Comm. on Intelligence*, 114th Cong. 2 (Sept. 10, 2015) (statement of James R. Clapper, Dir. of National Intelligence) [hereinafter "*Worldwide Cyber Threats*"], https://fas.org/irp/congress/2015_hr/091015clapper.pdf ("Cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact."); Nicole Gaouette, *Intel chief: Presidential campaigns under cyber attack*, CNN.COM (May 18, 2016), http://www.cnn.com/2016/05/18/politics/presidential-campaigns-cyber-attack/ ("Clapper said in his decades-long career in intelligence, he doesn't 'recall a time when we've been beset by a wider array and more diverse array of threats and crises than we are today.'").

B. The Analogy to Cybersecurity Attacks

[10] As mentioned in the Introduction, the field of cybersecurity provides an analogy for deciding what types of remedies individuals should have about processing of their information by surveillance agencies. Many of us today are at least somewhat familiar with three types of cybersecurity precautions: (1) do not click on links in emails, because they might be phishing attacks; (2) update your antivirus software, so viruses will not infect your computer; and (3) have a good firewall, so attackers cannot get into your system. The idea I am suggesting is simple but I believe helpful – be cautious about creating a new vector of attack, such as individual remedies, into a protected system.

[11] One way to make the point is to ask the reader to imagine that you are the hostile actor. The thought experiment is to consider how the hostile actor could make use of the attack vector of individual remedies – what could the hostile actor learn, in what ways? The hostile actor could seek to gain information about the agency's sources and methods:

1. *Detect whether the agency is surveilling specific individuals.* The hostile actor can deploy Alice, Bob, Carlos, and others to send messages and make individual remedy requests. For the individuals whose messages were intercepted, the hostile actor learns specifically which individuals are under surveillance, and can draw inferences about what triggered those individuals' being under surveillance contrasted with those who were not.

2. *Detect surveillance selectors.* Alice could send a variety of messages with words or phrases she thinks might be selectors, and see which ones turn up in her individual remedy request. Information that Alice learns could be used to evade surveillance (avoid use of those selectors), or to feed strategic disinformation to the agency (use the selectors but tell the agency false information).

3. *Detect what channels are under surveillance.* As shown in the example, Alice might use a text service, Bob an email service, and Carlos a chat service. They then file access requests, and only Bob has a file. If so, then the hostile actor has learned something valuable – the email service is under surveillance, but the text and chat services appear not to be.[2]

4. *Unmask intelligence and counterintelligence agents.* During the Cold War, Soviet agents were discovered within Western intelligence agencies.[3] Alice could use her individual remedy to determine whether someone is assisting the agency's intelligence efforts. For instance, if Alice suspects an individual, Mallet, is sharing information with the agency, she could carefully feed that person sensitive information; if that information later turns up in Alice's file,

[2] Another possible inference is that Bob was under surveillance, but not Alice or Carlos. The hostile actor would thus have reason to conduct a series of probes, to test the hypotheses about the agency's sources and methods.
[3] JOHN EARL HAYNES AND HARVEY KLEHR, VENONA: DECODING SOVIET ESPIONAGE IN AMERICA (2000).

then she has gained evidence that Mallet is working with the agency. The hostile actor could then take action against Mallet, or could try to "turn" Mallet in order to feed incorrect information back to the agency.

[12] These examples illustrate how individual access requests by Alice and her colleagues could harm the intelligence agency's efforts to protect national security. Using the analogy to cybersecurity, the individual access request becomes a tool for probing the agency's defenses – access requests can "map" the agency's system the way that a hacker maps the computer systems under attack.

[13] Harms to the intelligence agency's activities can also occur if the individual remedy is indirect. Rather than allowing Alice to gain access to the intelligence agency's files, the access might be given to someone on Alice's behalf. For instance, the individual remedy might allow access by a data protection official, Danielle. This indirect approach would limit the number of persons with access to classified information held by the intelligence agency. This approach has the potential to provide an individual remedy for Alice, while reducing Alice's ability to gain inferences about the agency's source and methods.

[14] Providing access to the data protection official, Danielle, would nonetheless have certain risks:

1. *Moving classified information to an unclassified database has security risks.* To protect national security, classified information is only properly protected if: (a) the person accessing the information has a security clearance; and (b) the information is housed in a classified system. Moving classified information to an unclassified database thus is prohibited, and carries risk, unless there is an explicit and justified decision that the disclosure would no longer harm national security.

2. *The data protection official's system becomes a target for hostile actors.* If Danielle moves information about Alice to the data protection agency, then Danielle's system becomes a prime target for attack. Data protection agencies, and other non-military and non-intelligence systems, do not generally receive the resources to protect against determined attacks by nation-state actors.[4] This sort of cyberattack by nation states on non-intelligence actors became widely visible in 2016, with news reports about attacks against targets such as the Democratic National Committee and Hillary Clinton's campaign manager.[5] The possibility of a hack or breach is relevant to the overall

[4] European experts have expressed concerns about lack of adequate staffing and financial resources for data protection agencies, who sometimes "are not in a position to carry out the entirety of their tasks because of the limited economic and human resources available to them." European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities*, 42 (2010), http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf; *Worldwide Cyber Threats*, *supra* note 1, at 3-4 (describing the risks and capabilities of state actors).

[5] *See* Nicole Gaouette, *Intel chief: Presidential campaigns under cyber attack*, *supra* note 1.

assessment of sending classified information into non-classified systems, such as to a data protection agency due to individual remedy requests.

3. *The data protection officials themselves become targets for hostile actors.* Again, considering the Cold War history of Soviet agents in Western intelligence agencies, there is the possibility that individuals such as Danielle could become targets for the hostile actors. Western intelligence agencies would face risks that a data protection official might reveal information due to sincere belief; for instance, individuals might believe they were principled whistleblowers, and decide to reveal classified information outside of lawful channels. There are also other ways that an official could be compromised, leading to disclosure of classified information.[6]

C. Risks of Revealing National Security Information

[15] In summary on the analogy to cyber-attacks, there are national security risks in creating a mechanism that reveals information held by the intelligence agency. Under US law, information is considered "top secret" if there would be "exceptionally grave damage" to national security if made publicly available.[7] Beyond "top secret," information held in US intelligence agencies is often "compartmentalized," with access only by individuals with a "Top Secret/Special Compartmentalized Information" security clearance. Intelligence information about named individuals is often, in my experience, available only to those with a TS/SCI clearance.[8]

[16] This extremely strict handling of personally identifiable information in the intelligence context is, in part, a privacy protection for the individual – there are strict limits on access to data about individuals who are not involved in the investigation of a crime, but whose information may arise during an intelligence investigation. The strict handling, in addition, is due to awareness of the risks to national security and the individual if the data becomes public. For instance, the information may be about someone cooperating with the US or an ally, but where the individual would be subject to harm if his identity was revealed. In terms used in Article 8 of

---

[6] I am not saying that there is any particular reason to believe that data protection officials would improperly disclose information. Instead, my point is that the history of intelligence agencies shows the possibility that the hostile actors will find ways to gain information unlawfully.

[7] *See* [2 PRINCIPLES FOR CLASSIFICATION OF INFORMATION] ARVIN S. QUIST, SECURITY CLASSIFICATION OF INFORMATION, *Ch. 7 Classification Levels* (1993) [hereinafter "SECURITY CLASSIFICATION OF INFORMATION"], https://fas.org/sgp/library/quist2/chap_7.html. In citing US law that states that an item marked "top secret" means that disclosure would cause "exceptionally grave challenge," I am not stating a view that every document marked "top secret" deserves "top secret" clearance. There is a considerable literature supporting the view that "over-classification" occurs in the US. *See, e.g.*, Dana Carver Boehm, *Guantanamo Bay and the Conflict of Ethical Lawyering*, 117 PENN ST. L. REV. 283 (2012); Alexandra Cumings & Kaplan v. Conyers, *Preventing the Grocery Store Clerk from Disclosing National Security Secrets*, 119 PENN ST. L. REV. 553 (2014); Jason B. Jones, *The Necessity of Federal Intelligence Sharing with Sub-Federal Agencies*, 16 Tex. Rev. L. & Pol. 175 (2011). My point, instead, is that there is national security risk in creating a system that permits outside individuals to probe the intelligence agency, revealing sensitive agency sources and methods.

[8] *See* SECURITY CLASSIFICATION OF INFORMATION, *supra* note 7, at *Appendix E Classification of Intelligence Information*.

the European Convention on Human Rights, such disclosures via an individual remedy could implicate the "rights and freedoms of others" if the data is revealed.

[17] In light of the strict control about access to intelligence information about a named individual, providing an individual remedy that gives outsiders access to that information raises national security risks. As discussed here, if the outside individual such as Alice can gain access to the information, then Alice and her colleagues can map the intelligence agency's activities. If a non-intelligence government employee can access the information, such as Danielle at the data protection agency, then Danielle would face a heightened risk of being subject to a nation-state level of attack. Consideration of the privacy advantages of such individual access should be weighed, in my view, with consideration of the national security risks as well.

II. The US State Secrets Doctrine

[18] Within the US, courts have established the state secrets doctrine to manage the usual rules for open judicial proceedings consistent with the risks to national security that can occur due to public disclosure. This section provides a brief overview of the doctrine. The purpose of the state secrets doctrine is to prevent litigation from disclosing sensitive material that could harm US national security. The doctrine requires the US government to state, through top level administration officials, that disclosure would threaten state secrets that would compromise national security. Courts examine the government's claim and independently determine – such as through *in camera* review of the material the government alleges to be harmful – whether disclosure in fact threatens American security interests. If the court agrees that a security threat exists, it excludes the material. The next Section of this Chapter describes similar doctrines in the EU.

A. Purpose of the State Secrets Doctrine

[19] The purpose of the state secrets doctrine is to protect national security, which would be endangered if information that could be used against the US were to be disclosed via judicial proceedings. A quote from the US Supreme Court illustrates the doctrine's national security focus:

> Many of the Government's efforts to protect our national security are well known. It publicly acknowledges the size of our military, the location of our military bases, and the names of our ambassadors to Moscow and Peking. But protecting our national security sometimes requires keeping information about our military, intelligence, and diplomatic efforts secret. We have recognized the sometimes-compelling necessity of governmental secrecy by acknowledging a Government privilege against court-ordered disclosure of state and military secrets.[9]

[9] *Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 484 (2011) (internal citations omitted). US Supreme Court cases may be found at https://www.supremecourt.gov/opinions/opinions.aspx, or https://supreme.justia.com/. Appellate decisions offer insight into the gravity of harms the state secrets doctrine is used to prevent. Litigation can reveal sensitive military secrets, such as classified weapons systems. *See Zuckerbraun v. Gen. Dynamics Corp*., 935 F.2d 544, 547–48 (2d Cir. 1991), https://scholar.google.com/scholar_case?case=8505678271071925191&q=935+F.2d+544&hl=en&as_sdt=80006

Conversely, the state secrets doctrine "may not be used to shield any material not strictly necessary to prevent injury to national security."[10]

B. Procedure for Invoking the State Secrets Doctrine

[20] The procedure for invoking the state secrets doctrine shows the care that US courts take before providing an exception to the usual rule of open proceedings. The US Supreme Court states that the state secrets doctrine "belongs to the [g]overnment and must be asserted by it;" the doctrine "can neither be claimed nor waived by a private party."[11] To assert a state secrets claim, leaders of executive branch agencies must review information at issue in litigation, identify the national security threats litigation poses, and formally submit their concerns to the court under oath. Specifically, the "head of the department which has control over" the matter being litigated must personally lodge a "formal claim of privilege" with the court.[12] Moreover, the agency head may only make a formal state secrets claim after "actual personal consideration of the matter."[13]

[21] US courts require state secrets claims to be detailed. "Simply saying 'military secret,' 'national security' or 'terrorist threat' or invoking an ethereal fear that disclosure will threaten our nation is insufficient" to support state secrets claims; instead, "[s]ufficient detail" must be provided for courts to make a "meaningful examination."[14]

C. Independent Judicial Evaluation of Executive State Secrets Claims

[22] When a US agency head makes a formal state secrets claim, US courts examine the government's submissions and independently determine that litigation presents an actual threat to national security. In this evaluation, the emphasis is on the court's independence – the court must "assess the validity of the claim of privilege, satisfying itself that there is a reasonable danger that disclosure of the particular facts in litigation will jeopardize national security."[15]

[23] To evaluate governmental state secrecy claims, the court may inspect evidence the government claims would harm national security if disclosed, or it may rely on the declaration of

---

(case involving "weapons systems aboard the U.S.S. Stark"). It can damage the US's intelligence capabilities, *e.g.*, by disturbing relationships with intelligence assets, or by revealing the sources and methods intelligence agencies are using. *See CIA v. Sims*, 471 U.S. 159, 175 (1985) (noting that disclosure of methods "may compromise the Agency's ability to gather intelligence as much as disclosure of the identities of intelligence sources").

[10] *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983), https://scholar.google.com/scholar_case?case=14501985049476297 41&q=709+F.2d+51&hl=en&as_sdt=80006.

[11] *United States v. Reynolds*, 345 U.S. 1, 7 (1953).

[12] *Id.* In practice, heads of US agencies – *e.g.* the Director of National Intelligence or Attorney General – submit a declaration that (a) outlines his or her review of the matter, (b) states his or her personal knowledge, and (c) explains with particularity the harms to national security he sees resulting from the disclosure of sensitive materials.

[13] *Id.* at 7-8. For a case rejecting the government's attempt to assert the state secrets doctrine because the agency director claiming the privilege did not "personally conside[r] the material for which the privilege is sought," *see Yang v. Reno*, 157 F.R.D. 625, 634 (M.D. Pa. 1994).

[14] *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007), https://scholar.google.com/scholar_case?case=5006140604567331133&q=507+F.3d+1190&hl=en&as_sdt=80006.

[15] *Zuckerbraun*, 935 F.2d at 546.

the agency director.[16] Generally speaking, if evidence is essential to a party's case, an *in camera* inspection is conducted; if the government raises plausible and substantial allegations of danger, a court may rely on the government's declaration.[17]

[24] Case law requires US courts to scrutinize government state secrets claims in the interest of upholding democratic commitments to open judicial proceedings. The Supreme Court has stated that the doctrine is "not to be lightly invoked."[18] Courts must "critically [] examine instances of [the state secrets doctrine's] invocation" in order to "ensure that [it] is asserted no more frequently and sweepingly than necessary."[19] State secret decisions place courts under the "special burden" of ensuring "that an appropriate balance is struck between protecting national security matters and preserving an open court system."[20]

[25] Cases reflect US courts carefully examining attempts to invoke the state secrets privilege:[21] "We take very seriously our obligation to review [government state secrets claims] with a very careful, indeed a skeptical, eye, and not to accept at face value the government's claim or justification of privilege."[22] Moreover, the court "must scrutinize the claim of privilege more carefully when the plaintiff has 'made a compelling showing of need for the information in question.'"[23]

D. Further Proceedings after Successful State Secrets Claims

[26] If judges independently determine that litigation threatens to harm national security, US cases hold they must prevent that harm from occurring. Evidence posing a national security risk must be "completely removed from the case."[24] Thus, when courts determine that state secrets must be kept out of proceedings, they must also determine "how the matter should proceed in light of the successful privilege claim."[25] In many cases, proceedings will go forward without

---

[16] The court's procedure is guided by the principle of not "forcing a disclosure of the very thing the [state secrets] privilege is designed to protect." *See Reynolds*, 345 U.S. at 8.
[17] *See Ellsberg*, 709 F.2d at 58–59 ("[T]he more compelling a litigant's showing of need for the information in question, the deeper the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate.") (internal citations and quotation marks omitted).
[18] *Reynolds*, 345 U.S. at 7.
[19] *Ellsberg*, 709 F.2d at 58.
[20] *Al-Haramain*, 507 F.3d 1203.
[21] For example: "We have spent considerable time examining the government's declarations (both publicly filed and those filed under seal). We are satisfied that the basis for the privilege is exceptionally well documented. Detailed statements underscore that disclosure of information concerning the Sealed Document and the means, sources and methods of intelligence gathering in the context of this case would undermine the government's intelligence capabilities and compromise national security. Thus, we reach the same conclusion as the district court: the government has sustained its burden as to the state secrets privilege." *Id.* at 1203-04.
[22] *Id.* at 1203.
[23] *In re Sealed Case*, 494 F.3d 139, 144 (D.C. Cir. 2007) (quoting *Ellsberg*, 709 F.2d at 59 n. 37, 61), https://scholar.google.com/scholar_case?case=15677361886209895 08&q=494+F.3d+139&hl=en&as_sdt=80006.
[24] *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998), https://scholar.google.com/scholar_case?case=4720850483028952155&q=133+F.3d+1159&hl=en&as_sdt=80006.
[25] *Al-Haramain*, 507 F.3d at 1202 (internal citation omitted).

the excluded evidence,[26] and can proceed to discovery and trial as long as plaintiffs can prove the "essential facts" of their claims "without resort to material touching upon military secrets."[27] In some cases, however, a successful state secrets claim can lead to dismissal of the proceedings or of certain claims.[28]

III. Similar State Secrets and Public Interest Doctrines in EU Member States

[27] Similar to the US state secrets doctrine, EU Member States have established doctrines to prevent national security information from being disclosed in litigation. I present summaries of my research, alphabetically, for: (A) French statutes criminalizing use of classified information in court proceedings; (B) the German governmental secrecy objection; (C) Irish privilege doctrines relevant to the security of the state; (D) the Italian state secrets privilege; and (E) the United Kingdom's doctrine of public interest immunity.

[28] The similarity of these US and EU doctrines, in my view, puts into perspective the earlier discussion of the risks of hostile actors using individual remedies to learn the secrets of US and EU intelligence agencies. The discussion about the cybersecurity style attacks by hostile actors illustrated national security risks from granting access by individuals to intelligence agency information. The discussion about US and EU state secret doctrines show a basic similarity of how courts are aware of the risk of revealing national security secrets, and limit the ability of litigants to use individual remedies to compromise national security.

A. France: Criminal Sanctions for Disclosing State Secrets in Court

[29] French statutes create criminal penalties for accessing or disclosing classified information in judicial proceedings. Under France's Defense Code, individual executive agencies (such as

---

[26] "The effect of the government's successful invocation of the state secrets privilege . . . is well established: '[T]he result is simply that the evidence is unavailable, as though a witness had died, and the case will proceed accordingly, with no consequences save those resulting from the loss of the evidence.'" *Ellsberg*, 709 F.2d at 64 (quoting 2 McCormick on Evidence § 233 (E. Cleary ed. 1972)).

[27] *Al-Haramain*, 507 F.3d at 1204 (quoting *Reynolds*, 345 U.S. at 11).

[28] Decisions recognize that in rare cases, "the very subject matter of the action" is a state secret, *see Reynolds*, 345 U.S. at 11 n.26 (citing *Totten v. United States*, 92 U.S. 105 (1875)), or that state secrets are "so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters," *Fitzgerald v. Penthouse Int'l, Ltd*., 776 F.2d 1236, 1241-42 (4th Cir. 1985), https://scholar.google.com/scholar_case?case=3765361197667528388q=776+F.2d+1236&hl=en&as_sdt=80006. In such cases, the court has discretion to dismiss proceedings in full or in part. Courts have done so, for example, when individual litigation would require the government to identify the location of nuclear weapons. *See Weinberger v. Catholic Action of Hawaii/Peace Educ. Project*, 454 U.S. 139 (1981). Also, a case challenging a program under Section 702 of FISA has been dismissed because the court determined it would "risk informing adversaries of the specific nature and operational details" of the program. *Jewel v. Nat'l Sec. Agency*, No. C 07-00693 JSW, 2015 WL 545925, at *5 (N.D. Cal. Feb. 10, 2015), http://www.leagle.com/decision/In%20FDCO%2020150211A45/Jewel%20v.%20National%20Security%20Agency. In these rare cases, US courts describe dismissal as "ultimately the less harsh remedy" because it vindicates "the greater public good" of protecting the nation and its citizens. *Bareford v. Gen. Dynamics Corp*., 973 F.2d 1138, 1144 (5th Cir. 1992), https://scholar.google.com/scholar_case?case=7680050268108144567&q=973+F.2d+1138&hl=en&as_sdt=80006, opinion vacated in part on denial of reargument (Oct. 14, 1992).

the Ministry of Defense) are responsible for classifying information.[29] Article 413-9 of France's Penal Code declares classified information to constitute national defense secrets.[30] Accessing, learning the content of, reproducing, or making defense secrets public is a crime punishable by five years' imprisonment or a fine of € 75,000.[31]

[30] Judges may not access or use defense secrets in judicial proceedings, nor may parties disclose them, unless the secrets are first declassified – otherwise, the judge or disclosing party commits a crime under Article 413 of France's Penal Code.[32] Instead, France's Law No. 98-567 creates a Consultative Commission on National Defense Secrets (CCNDS).[33] When a court encounters classified materials and wishes to declassify them for use in judicial proceedings, it can petition the CCNDS for a classification review.[34] The CCNDS will issue a recommendation as to whether the documents at issue should remain secret. However, the ministry or agency that originally classified the information is not bound by the CCNDS's declassification recommendation.[35] It may continue to refuse to declassify materials.[36] As a result, unless executive agencies agree to declassify materials sought to be used in court, French law effectively excludes the materials from use in judicial proceedings.[37]

---

[29] *See* CODE DE LA DÉFENSE [DEFENSE CODE], particularly at Arts. R.*1132 *et seq.* (Fr.), (in French) https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307.

[30] *See* CODE PÉNAL [PENAL CODE], Art. 413-9, (in French) https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006418400.

[31] *Id.* at Art. 413-11.

[32] *See id.* at Arts. 413-9-413-11.

[33] *See* Loi 98-567 du 8 juillet 1998 instituant une Commission consultative du secret de la défense nationale [Law of 8 July 1998 Instituting a Consultative Commission on National Defense Secrets], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [OFFICIAL GAZETTE OF FRANCE] July 9, 1998, p. 10488, Art. 1 [hereinafter "CCNDS Law"], (in French) https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000389843&categorieLien=id.

[34] *Id.* Art. 4.

[35] *See* MINISTÈRE DE LA DÉFENSE [DEFENSE MINISTRY], SECRÉTARIAT GÉNÉRAL POUR L'ADMINISTRATION [SECRETARY-GENERAL FOR ADMINISTRATION], *Secret Défense* [Defense Secrets] (Sept. 17, 2012), (in French) http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/secret-defense/secret-defense (noting that the CCSND's declassification recommendations are not binding on ministries).

[36] The CCNDS's recommendations are published in France's Official Journal independent of whether the ministry elects to follow them. *See* CCNDS Law, *supra* note 33, Art. 8.

[37] France's Constitutional Council has held that the prohibition on judges accessing classified materials is unconstitutional as applied to a magistrate who, in the course of exercising his duty to investigate facts, accesses a classified physical area. *See* Conseil Constitutionnel [CC] [Constitutional Council], decision No. 2011-192 QPC, Nov. 10, 2011, at para. 37 ("*Ekaterina*"), (in English) http://www.conseil-constitutionnel.fr/conseil-constitutionnel/english/case-law/decision/decision-no-2011-192-qpc-of-10-november-2011.104102.html. The Council, however, deemed the remainder of the classification regime described above to be constitutional. *See id.* at para. 28 *et seq.*

B. Germany: the Governmental Secrecy Objection

[31] Germany has codified a governmental secrecy doctrine in Section 99 of the Code of Administrative Court Procedure (CACP) (*Verwaltungsgerichtsordnung*).[38] This provision permits government agencies to refuse to produce any documents or information that (a) "would prove disadvantageous to the interests of the Federation or of a [State]," or that (b) "must be kept strictly secret in accordance with a statute" or "due to their essence."[39] German court decisions require courts to examine *in camera* materials over which government entities claim secrecy.[40] In response, the German legislature enacted *in camera* review procedures that show concern for litigation against the government becoming an avenue for revealing state secrets:

- Once a government agency has raised national security objections to production, the party seeking the documents or information may lodge a motion for *in camera* review.

- The trial court does not conduct the *in camera* review. Instead, if a top level federal agency (such as the Ministry of Defence) contends that disclosing information would harm Germany's national security, Germany's Supreme Administrative Court (SAC) – the court of last resort in the administrative court system – conducts the *in camera* review via an interlocutory proceeding.[41]

- The SAC has created a Special Panel (*Fachsenat*) to conduct *in camera* reviews of sensitive evidence.[42] The Special Panel's rulings are final, and no appeal is permitted.[43]

---

[38] In Germany, suits against the government or a federal or state agency must generally be filed in the administrative courts. Accordingly, the CACP contains the rules by which government agencies can keep sensitive information out of public court proceedings.

[39] VERWALTUNGSGERICHTSORDNUNG, [VWGO] [CODE OF ADMINISTRATIVE COURT PROCEDURE] § 99(1) [hereinafter "CACP"], (in English) https://www.gesetze-im-internet.de/englisch_vwgo/englisch_vwgo.html.

[40] Until the 1990s, courts were permitted to rely on agency assertions that evidence was potentially harmful and should not be disclosed. In 1999, the German Constitutional Court required that administrative courts conduct *in camera* review of the material. *See* BVerfG [Federal Constitutional Court], decision of the First Senate of 27 October 1999, 1 BvR 385/90, (in German) https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1999/10/rs19991027_1bvr038590.html.

[41] Both the German government as well as its administrative court system are arranged along federal lines. If a state agency, or a lower-level federal agency, invokes a secrecy claim, the interlocutory *in camera* review is first conducted by a special panel of the Administrative Court of Appeal (*Oberverwaltungsgericht*) in the German state where proceedings are pending; its decision can be appealed to the SAC's Special Panel. If a top-level federal agency – such as the Ministry of Defence, Interior Ministry, etc. – invokes public interests (such as national security) against production, the interlocutory *in camera* review goes directly to the SAC. The secrecy requirements outlined in this section apply to both types of *in camera* proceedings. *See* CACP, *supra* note 39, at § 99(2).

[42] For a decision of the SAC Special Panel, *see, e.g.*, BVerwG [Supreme Administrative Court], judgment of 26 August 2004, BVERWG 20 F 19.03, (in German) http://www.bverwg.de/entscheidungen/entscheidung.php?ent=260804B20F19.03.0. In this decision, the Special Panel notes that the German legislature designed the *in camera* proceedings of CACP § 99 to minimize the number of persons who gain access to potentially sensitive materials. For the same reason, the court states that each German administrative appellate court obligated to conduct Section 99 *in camera* reviews created "only one" special panel. *Id.* at para. 7.

- Proceedings before the SAC's Special Panel are conducted in secret,[44] and all judges and court personnel are bound to maintain secrecy.[45] If the agency asserting privilege states that "special reasons of confidentiality or classification" are present, it can require review to be conducted within the agency's own offices.[46]

- The SAC's order resolving the privilege claim "may not provide an indication of the nature and content of the secret certificates, files, documents and information."[47]

[32] If the SAC determines that documents present a danger to German security that outweighs the interest in disclosure, the documents are barred from being used in the underlying court proceedings. In addition to documentary evidence, German agencies can prohibit individuals from testifying on sensitive matters – and if the SAC finds that testimony would harm national security, it can prohibit plaintiffs from testifying on their own behalf to the extent it would touch on sensitive matters.[48] If evidence or testimony is essential to a claim, SAC exclusion decisions can lead to a dismissal or other form of adverse judgment.

C. Irish Privilege Doctrines relevant to the Security of the State

[33] In Ireland, courts apply doctrines of public interest privilege and statutory privilege in situations where "the vital interests of the State (such as the security of the State)" may be harmed through information disclosed in judicial proceedings.[49] Public interest privilege is a claim that – with regard to documents at issue in litigation – the public's general interest in open proceedings is outweighed by another public interest of higher order, such as State security.[50] Statutory privilege is an assertion that a statute prohibits disclosure, such that a statutorily recognized public interest justifies keeping certain documents or information confidential.[51]

---

[43] CACP, *supra* note 39, at § 99(2).
[44] *Id.*, 7th sentence.
[45] *Id.*, 10th sentence.
[46] *Id.*, 8th sentence.
[47] *Id.*, 10th sentence.
[48] For an example of the Special Panel upholding an agency-imposed prohibition on testifying on sensitive matters, *see* BVerwG [Supreme Administrative Court], Judgment of 26 August 2004, BVERWG 20 F 19.03, (in German) http://www.bverwg.de/entscheidungen/entscheidung.php?ent=260804B20F19.03.0.
[49] *See Murphy v. Corporation of Dublin* [1972] IR 215, 283 (S.C.) ["*Murphy*"].
[50] *See, e.g., Livingstone v. Minister for Justice* [2004] IEHC 58 at § 6 (H. Ct.), http://www.bailii.org/ie/cases/IEHC/2004/58.html, (describing public interest privilege as a balancing of "the public interest in the proper administration of justice by making all relevant material available to litigants, and the public interest in not harming society as a whole by releasing highly confidential State information in respect of which public interest immunity is claimed").
[51] Statutory privilege appears to have been first recognized in *Cully v. Northern Bank Finance Corp.* [1984] ILRM 683, and more recently applied in *O'Brien v. Ireland* [1995] 1 IR 568 (H.C.).

[34] Public interest or statutory privilege claims must be asserted by "the person seeking the privilege;"[52] in the context of litigation posing risks to State security, government ministers and An Garda Síochána officers of appropriate rank have asserted such privilege claims.[53] Like in the US, Irish courts "closely scrutinise"[54] the claim and independently determine whether the general interest in open proceedings is in fact outweighed by a weightier public interest, such as State security.[55] In making this determination, courts may examine the documents over which privilege has been claimed. At the same time, "[t]here is no obligation on the judicial power to examine any particular document," and courts "can and will in many instances uphold a claim of privilege in respect of a document merely on the basis of a description of its nature and contents."[56]

[35] Irish courts have applied public interest and statutory privileges to prevent sensitive information from being disclosed in cases implicating significant security interests. The Supreme Court's decision in *Murphy v. Corporation of Dublin* states that courts should intervene in litigation to preserve national security,[57] and permit even the existence of documents to be withheld when serious harm is threatened.[58] Further cases have stated that in general, litigation should not disclose confidential information about An Garda Síochána's sources,[59] methods,[60] or ongoing investigations.[61] In *Keating v. Radio Telefís Éireann*, the High Court refused to permit inspection or discovery of documents relating to An Garda's witness protection program, finding that doing so would harm "the prevention and detection and prosecution of crime" and would "put at risk the lives and wellbeing of the individuals" involved in the program.[62] Additionally, in *O'Brien v. Ireland*, the High Court refused to permit an Irish soldier's widow from discovering court of inquiry reports about his death during a UN peacekeeping mission, after the

---

[52] *McLoughlin v. Aviva Insurance (Europe) Public Ltd. Co.* [2011] IESC 42 (Transcript), http://www.bailii.org/ie/cases/IESC/2011/S42.html.

[53] *See, e.g.*, *Keating v. Radio Telefís Éireann* [2013] IEHC 393, http://courts.ie/Judgments.nsf/0/8CF48D7FA15CB2A080257BD4004CF393, for an example of affidavits claiming public interest privilege submitted by Garda officers.

[54] *Id.*

[55] *Ambiorix Ltd. v. Minister for the Environment* [1992] 1 I.R. 277, 283 (S.C.) ("Where a conflict arises during the exercise of the judicial power between the aspect of public interest involved in the production of evidence and the aspect of public interest involved in the confidentiality or exemption from production of documents . . . , it is the judicial power which will decide which public interest shall prevail.").

[56] *Id.* at 284.

[57] *Murphy* [1972] I.R. at 283-284 ("It is clear that, when the vital interests of the State (such as the security of the State) may be adversely affected by disclosure or production of a document, greater harm may be caused by ordering rather than by refusing disclosure or production of the document.").

[58] *Id.* ("[I]n certain circumstances the very disclosure of the existence of a document, apart altogether from the question of its production, could in itself be a danger to the security of the State.").

[59] *See Skeffington v. Rooney* [1997] 1 IR 22 (S.C.) (the "countervailing public interest [] in the detection and prevention of crime [] has led the courts . . . to allow the anonymity of police informers to be preserved").

[60] *See Breathnach v. Ireland* [1993] 2 IR 458 (H.C.) ("[T]here may be material the disclosure of which would be of assistance to criminals by revealing methods of detection or combatting crime," which is "a consideration of particular importance today when criminal activity tends to be highly organised and professional.").

[61] *See McLoughlin* [2011] IESC 42 at para. 12 (Transcript) ("[I]n general documents material to an ongoing criminal investigation by An Garda Síochána should not be required to be disclosed in civil proceedings.").

[62] *Keating* [2013] IEHC 393.

government asserted that permitting discovery "may endanger not only the Irish battalion, but the United Nations peace-keeping force generally."[63]

[36] In addition to case law, provisions in Ireland's Criminal Justice (Surveillance) Act, 2009 (CJA)[64] show hesitancy to disclose information about Irish surveillance in judicial proceedings. Under Section 15 of the CJA, "the existence or non-existence" of surveillance or facts related to it "shall not be disclosed by way of discovery or otherwise in the course of any proceedings."[65] Courts "shall not authorize" disclosure of such information if doing so is likely to create a material risk to (a) "the security of the State;" (b) counterterrorism activities; or (c) the "integrity, effectiveness and security" of Garda or Irish Defence Forces operations.[66] Courts may only authorize disclosure of surveillance-related information if "in all of the circumstances it is in the interests of justice to do so," and "subject to such conditions as [the court] considers justified."[67]

D. Italy: the State Secrets Privilege

[37] Within Italy, statutory rules and court decisions ensure that matters designated as state secrets will not be disclosed through judicial proceedings. Italian statutes prohibit "public officials, public employees and public service providers" from disclosing information that has been classified as a state secret in court proceedings.[68] When a state secrecy objection is raised, the court must determine whether the evidence at issue is essential to the proceedings. If it is, the court must (a) stay any proceedings that could disclose secret matters, and (b) request the Italian Prime Minister to confirm "the existence of State secret status" over the materials at issue.[69] The Prime Minister has 30 days to respond via a reasoned explanation.[70]

[38] If the Prime Minister confirms state secrets are in fact threatened with disclosure, the trial court may elect to exclude the secret material and, depending on its importance, dismiss the proceedings.[71] Alternatively, the court may challenge the Prime Minister's secrecy classification by ordering an interlocutory appeal to Italy's Constitutional Court.[72] The Constitutional Court,

---

[63] *O'Brien v. Ireland* [1995] 1 IR 568 (H.C.). The Court held the court of inquiry reports were covered by statutory privilege. *See id.* (citing the Diplomatic Relations and Immunities Act, 1967; the Defence Act, 1954; and the Defence Forces Rules of Procedure, 1954).

[64] *See* Criminal Justice (Surveillance) Act 2009 (Act. No. 19/2009) (Ir.), http://www.irishstatutebook.ie/eli/2009/act/19/section/15/enacted/en/html#sec15.

[65] *Id.* § 15(1).

[66] *Id.* § 15(2).

[67] *Id.* § 15(3).

[68] Legge 124/2007: Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto [Law no. 124/2007: System of Intelligence for the Security of the Republic and New Provisions on Secrecy] § 41(1) (It.) [hereinafter "Italian Intelligence & Secrecy Law"], (in English) https://www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html. "State secrets" are defined as information whose disclosure "may be used to damage the integrity of the Republic (including in relation to international agreements, the defence of its underlying institutions as established by the Constitution, the State's independence vis à vis other states and its relations with them, as well as its military preparation and defence)." *Id.* § 39(1). The Prime Minister is responsible for classifying matters as state secrets. *See id.* § 39(5).

[69] *Id.* § 41(2).

[70] *Id.* § 41(4), (5).

[71] *Id.* § 41(3).

[72] *Id.* § 41(8).

however, has stated it will not review the Prime Minister's secrecy classification on the merits, *i.e*. it will not decide whether the information is properly classified. The Constitutional Court has interpreted its duty narrowly, as limited to confirming that the Prime Minister has followed the statutory procedure for claiming secrecy over the materials at issue.[73] The court explains its refusal to examine secrecy claims as follows: "the choice of the necessary and appropriate means to ensure national security is a political one, belonging, as such, to the Executive branch and not to the ordinary judiciary."[74] As a result, the executive's assertion of state secrecy will likely bind the Italian courts.

[39] A successful state secrecy objection prohibits the Italian court "from acquiring or using the information having State secret status even indirectly."[75] Although the court is not prohibited from proceeding on the basis of "elements existing separately and independently of the records, documents or matters having State secret status,"[76] if secret evidence is essential to the claims, "the judge shall state that he/she cannot proceed on account of the existence of a State secret."[77]

E. United Kingdom: the Public Interest Immunity Doctrine

[40] In the United Kingdom, courts apply the doctrine of public interest immunity (PII) as a response to litigation that threatens to disclose information that could harm national security. PII is a claim that given the sensitive nature of particular documents, "it would be injurious to the public interest" to disclose them or produce them for inspection.[78] If a PII claim is successfully asserted, evidence is excluded from litigation.

[41] Similar to the US approach, PII claims must be asserted by the UK government. To assert a PII claim, the minister with responsibility for the information in question submits a certificate to the court detailing why disclosure or production would harm the UK's interests.[79] UK courts then independently determine whether, with regard to the documents at issue, higher order public interests (such as national security) outweigh the interest in open judicial proceedings. To make this determination, UK courts may inspect the documents over which the government has claimed privilege.[80]

---

[73] *See* Corte Constituzionale [Constitutional Court], 11 marzo 2009, Judgment 106/2009 ("*Abu Omar*") (adopting limited review of the Prime Minister's secrecy assertions), (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2009&numero=106; Corte Constituzionale [Constitutional Court] 29 febbraio 2012, Judgment 40/2012 ("*Abu Omar*") (affirming 2009 ruling), (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2012&numero=40; Corte Constituzionale [Constitutional Court] 19 febbraio 2014, Judgment 24/2014 ("*Abu Omar*") (reaffirming 2009 ruling), (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2014&numero=24.

[74] *See* Corte Constituzionale [Constitutional Court], 11 marzo 2009, Judgment 106/2009 ("*Abu Omar*"), at para. 3, (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2009&numero=106.

[75] Italian Intelligence & Secrecy Law, *supra* note 68, at § 41(5).

[76] *Id.* § 41(6).

[77] *Id.* § 41(3).

[78] *Duncan v. Cammel Laird & Co. Ltd.* [1942] AC 624, 627 (H.L.) (UK), http://www.bailii.org/uk/cases/UKHL/1942/3.html.

[79] *Id.* at 638.

[80] *Conway v Rimmer* [1968] AC 910 (H.L.) (UK), http://www.bailii.org/uk/cases/UKHL/1968/2.html.

[42] In cases where litigation threatens national security, UK courts have held that they should afford deference to the executive's claim of privilege and may need to avoid *in camera* inspections, because evaluating the national security implications of documents goes beyond the judiciary's traditional expertise.[81] Thus, in national security cases, evidence should be excluded as long as the minister's certificate substantiates an actual or potential risk to UK security.[82]

[43] As an alternative to asserting a PII claim, UK law has recently provided the option of requesting the court to hold a Closed Material Proceeding (CMP).[83] In a CMP, evidence that would otherwise be excluded via a PII claim is instead evaluated by the court in a secure, "closed" proceeding.[84] Special Advocates are appointed to represent the interests of non-governmental parties.[85] The court then issues a ruling or judgment that adjudicates the parties' rights, but does not disclose classified information.[86] The purpose of a CMP is to provide a judicial determination based on evidence – as opposed to a dismissal due to a PII claim – while making sure that information that could be used to harm UK interests is not disclosed.

---

[81] *See, e.g., Balfour v. Foreign and Commonwealth Office* [1993] ICR 663 (E.A.T.) (UK), http://www.bailii.org/uk/cases/UKEAT/1993/182_92_1210.html: "[There are] two separate categories of situations where the public interest is involved. The first [is] where the reasons given are susceptible of being weighed by judicial experience, and there the judge has to do the weighing or balancing process which usually involves an inspection by him[;] and the second [is] where the reasons given by the Minister are of a character which judicial experience is not competent to weigh. In the latter case, the judge by definition has no effective means for weighing the reasons adduced but it is still his function to perform the balancing act between the two public interests, one of the proper administration of justice which requires relevant evidence to be disclosed and not hidden, the other the protection of national security. [I]t will be the latter that will prevail, if . . . evidence of the necessary factual link between the documents and the reasons adduced is produced."

[82] *See Balfour v. Foreign and Commonwealth Office* [1994] 2 All ER 588, [1994] 1 W.L.R. 681, 688 (C.A.) (UK) ("There must always be vigilance by the courts to ensure that public interest immunity of whatever kind is raised only in appropriate circumstances and with appropriate particularity, but once there is an actual or potential risk to national security demonstrated by an appropriate certificate the court should not exercise its right to inspect.")

[83] *See* Justice and Security Act 2013 c. 18 (UK) [hereinafter "JSA"], http://www.legislation.gov.uk/ukpga/2013/18/pdfs/ukpga_20130018_en.pdf. Under the JSA, CMPs are available for civil, immigration, and employment proceedings.

[84] The court may invoke CMPs whenever it finds that (a) a party would be required to disclose "material the disclosure of which would be damaging to the interests of national security" during proceedings; and (b) the interests of justice favor proceeding via CMP. *See* JSA §§ 6(4), (5), (11).

[85] *See* JSA § 9. To protect secrecy, parties represented by a Special Advocate do not know who the advocate is, nor is the advocate "responsible to the party to the proceedings whose interests the person is appointed to represent." JSA § 9(4).

[86] Depending on the kind of rights the court is adjudicating, European Court of Human Rights decisions that have been adopted by the English courts may require it to provide the 'gist' of its reasoning to an affected individual.

IV. US Criminal Proceedings under the Classified Information Procedures Act

[44] The US Classified Information Procedures Act (CIPA) protects criminal defendants' rights while preventing disclosure of classified national security information.[87] As with the US systemic safeguards for foreign intelligence investigations, CIPA provides two important protections: (1) supervision by an independent judge; and (2) access by the judge and other participants to classified information, without disclosing classified information publicly.

[45] CIPA is designed to "protec[t] and restric[t] the discovery of classified information in a way that does not impair the defendant's right to a fair trial."[88] CIPA governs criminal proceedings where classified information may be disclosed.[89] CIPA is not designed to change defendants' substantive rights; instead, it is a "procedural framework for ruling on questions of admissibility involving classified information before introduction of the evidence in open court."[90]

[46] This section outlines criminal proceedings under CIPA. CIPA applies when the court enters a protective order governing how parties are to handle classified information during proceedings. The government must then satisfy constitutional and statutory discovery obligations, potentially – subject to court approval – producing substitutes for some items of classified evidence. After discovery, the defense must give notice of the classified information it anticipates using at trial. This results in a hearing at which the court determines which classified items are admissible as evidence. The government can then ask the court for permission to use substitutes of classified items the court has deemed admissible. If the court refuses, the government must either permit disclosure or suffer an adverse order.

A. Protective Order

[47] CIPA applies when the government asks the court to enter a protective order for classified information. Pursuant to CIPA, the US Judicial Branch has adopted security procedures for protecting classified information in federal courts.[91] The court enters a protective

---

[87] CIPA is codified at 18 U.S.C. App. III §§ 1-16, and is available in its entirety at https://www.law.cornell.edu/uscode/html/uscode18a/usc_sup_05_18_10_sq3.html.

[88] *United States v. O'Hara*, 301 F.3d 563, 568 (7th Cir. 2002), https://scholar.google.com/scholar_case?case=2763159407792597911&q=301+F.3d+563&hl=en&as_sdt=80006. CIPA also attempted to alleviate "the growing problem of greymail," *i.e*. "a practice whereby a criminal defendant threatens to reveal classified information during the course of his trial in the hope of forcing the government to drop the criminal charge against him." *United States v. Anderson*, 872 F.2d 1508, 1514 (11th Cir. 1989), https://scholar.google.com/scholar_case?case=12402375278722086310&q=872+F.2d+1508&hl=en&as_sdt=80006.

[89] Classified information is defined as "any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security." CIPA § 1(a), codified at 18 U.S.C. App. III § 1(a).

[90] *Anderson*, 872 F.2d at 1514.

[91] Section 9 of CIPA required the Chief Justice of the US Supreme Court to "prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States." CIPA § 9(a), codified at 18 U.S.C. App. III § 9(a). The security procedures currently in force are codified at 18 U.S.C. App. III § 9 note (issued Feb. 12, 1981) [hereinafter "Judicial Branch Security Procedures"].

order consistent with these procedures, to govern how classified information is handled during the case.[92]

[48] The Judicial Branch's security procedures generally require defense attorneys to obtain a security clearance in order to receive and view classified information.[93] The court gives defense attorneys an opportunity to apply for security clearances if they do not yet have one. The court also appoints a member of the US Department of Justice's Management Division as a Court Security Officer (CSO),[94] to assist defense attorneys in obtaining appropriate clearances. Upon receiving security clearances, defense lawyers can review the relevant classified information.[95]

B. Discovery

[49] After entry of a protective order, CIPA cases move to the discovery phase. As with other US criminal proceedings, the prosecution is subject to discovery obligations, such as producing exculpatory evidence (evidence that tends to weaken the prosecution's case).[96] CIPA does not change the scope of these discovery obligations,[97] but introduces a court-mediated procedure for production. The court inspects the submitted evidence *in camera* and determines what evidence is discoverable.[98]

[50] Classified items the court deems discoverable are produced to the defense. The government, however, may argue that national security would be harmed if particular items were produced, and propose substitutes for those items.[99] The court then determines whether the government has made a "sufficient showing,"[100] and may approve substitutes of classified evidence to be produced.[101] CIPA permits substitutes such as: (a) summaries of information from classified documents; (b) admissions of facts classified evidence would prove; or

---

[92] *See id.* § 3. The government must request the protective order by filing a motion that sets forth the national security concerns the case raises. If the government requests a protective order, CIPA requires the court to issue it. *See id.*

[93] *See* Judicial Branch Security Procedures, *supra* note 91.

[94] *See id.* § 2 ("In any proceeding in a criminal case . . . in which classified information is within, or reasonably expected to be within, the custody of the court, the court shall designate a court security officer.").

[95] If defense attorneys are unable to obtain a security clearance, they may seek an exemption order from the court. Alternatively, the court can permit a security cleared co-counsel to assist the defense.

[96] Exculpatory evidence is referred to as "*Brady* material" after the US Supreme Court case that required its production. *See Brady v. Maryland*, 373 U.S. 83 (1963). The Federal Rules of Criminal Procedure set forth additional categories of evidence the government must produce, including: (a) any item obtained from the defendant; (b) any item that the government intends to use for its case-in-chief against the defendant; and (c) any items that are "material to preparing the defense." *See* FED. R. CRIM. P. 16(a)(1)(E), https://www.law.cornell.edu/rules/frcrmp/rule_16.

[97] "[CIPA] creates no new rights of or limits on discovery of a specific area of classified information. Rather it contemplates an application of the general law of discovery in criminal cases[.]" *United States v. Yunis*, 867 F.2d 617, 621 (D.C. Cir. 1989), https://scholar.google.com/scholar_case?case=4751659880446145244&q=867+F.2d+617&hl=en&as_sdt=80006.

[98] Along with the evidence it submits for *in camera* discoverability review, the government may submit an *ex parte* brief arguing which evidence should or should not be found discoverable.

[99] *See* CIPA § 4, codified at 18 U.S.C. App. III § 4.

[100] *Id.*

[101] If the court denies the government's request to produce substitutes of classified information, its decision may be subject to interlocutory appeal. *See id.* § 7(a).

(c) redacted documents.[102] Additionally, the government may declassify information so that it can be produced to the defendant.

C. Pretrial Admissibility Proceedings

[51] Following the discovery process, CIPA provides pretrial procedures to determine what classified information will be admissible at trial. First, the defense specifies the classified materials it expects to use at trial. This leads to a hearing at which the court determines admissibility. Then, the government can ask the court for permission to use substitutes of classified materials. If the court refuses, the government must decide to permit disclosure or suffer an adverse order.

1. The Admissibility Hearing

[52] In CIPA cases, the defense provides notice of what classified information it intends to use (or cause to be used) at trial.[103] After receiving notice from the defense, or at the request of the government, the court holds a hearing. At the hearing, the court makes "all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding."[104]

[53] Prior to the hearing, the prosecution provides the defense with notice of the classified information it considers "at issue."[105] At the hearing, held *in camera*, the parties present arguments as to which items of classified information should be admissible.[106] The court applies generally applicable evidence rules to determine what classified items are admissible as evidence.[107] Under CIPA, the court uses "existing standards for determining relevance and admissibility of evidence."[108]

[54] For each item of classified evidence the court deems admissible, the court orders the prosecution to "provide the defendant with the information it expects to use to rebut the classified information."[109] If the government fails to provide rebuttal information, it can be excluded from the trial.[110]

---

[102] *Id.* § 4.
[103] *Id.* § 5(a).
[104] *Id.* § 6(a).
[105] *See id.* § 6(b)(1).
[106] The court can excuse government lawyers from the hearing while the defense makes a proffer of its case, to avoid divulging defense strategies to the prosecution.
[107] The Federal Rules of Evidence that generally govern admissibility determinations are available at https://www.law.cornell.edu/rules/fre.
[108] *Anderson*, 872 F.2d at 1514.
[109] CIPA § 6(f), codified at 18 U.S.C. App. III § 6(f). The court may also "place the [prosecution] under a continuing duty to disclose such rebuttal information."
[110] *Id.* ("If the [prosecution] fails to comply with its obligation [to provide rebuttal information], the court may exclude any evidence not made the subject of a required disclosure and may prohibit the examination by the [prosecution] of any witness with respect to such information.").

2. Government Requests to Use Substitutes

[55] Classified information the court finds to be admissible can be used as evidence at trial, and thus publicly disclosed. However – as in the discovery stage – CIPA permits the government to argue that national security requires using substitutes of classified materials that have been deemed admissible.[111]

[56] The court may permit government-offered substitutes to be used in lieu of original materials if it finds they "will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information" at issue.[112] CIPA anticipates substitutes such as (a) written summaries of classified information; (b) admissions of or stipulations to facts classified information would prove; or (c) documents where non-relevant classified information has been redacted.[113]

3. The Government's Right to Block Disclosure, and Mandatory Sanctions

[57] The court may find that a government-proffered substitute will not provide defendants with an adequate ability to defend themselves, and may thus deny the government's request to use substitute evidence.[114] If so, the defense has the right to disclose the classified material without alteration by presenting it as evidence at trial.

[58] In such situations, CIPA provides that the government decides whether it will permit classified materials to be disclosed, or block disclosure and suffer the consequences. If the government decides to let the defense disclose classified information, the case proceeds to trial. Alternatively, the government can block the disclosure of classified evidence. To do so, the US Attorney General files an affidavit objecting to the use of classified information; in that event, the court orders "that the defendant not disclose" the objected-to materials.[115]

[59] If the government objects to the use of classified information in this fashion, CIPA requires the court to dismiss the criminal proceedings unless it finds that "the interests of justice would not be served by dismissal."[116] If it finds the latter, the court enters an alternative: (a) dismissal of specific charges brought against the defendant; (b) conclusively resolving issues of fact against the government; or (c) striking all or part of a government witness's testimony.[117]

---

[111] *Id.* § 6(c).
[112] *Id.* § 6(c)(1).
[113] *See id.* §§ 6(c)(1), 8(b).
[114] When the court requires the government to let the defendant use classified information without alteration, the government may have a right to an expedited interlocutory appeal. Section 7(a) of CIPA permits interlocutory appeals when the trial court has entered an order "authorizing the disclosure of classified information." *Id.* § 7(a).
[115] *Id.* § 6(e)(1).
[116] *Id.* § 6(e)(2).
[117] *Id.* § 6(e)(2)(A)-(C). The court may also enter any sanction "the court determines is appropriate." *Id.* When the court enters sanctions, it must grant the government an opportunity to (a) seek an expedited interlocutory appeal, and to (b) withdraw its objection to the use of classified information at trial.

[60] In summary on CIPA, criminal defendants benefit from the statute's clear procedures for the treatment of classified information. Defendants retain their right to defend themselves in this process, even against classified evidence, and under full judicial supervision.

CHAPTER 9:

THE BROAD SCOPE OF "ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS" SUBJECT TO SECTION 702

[1] This Chapter describes US law relevant to determining the scope of what organizations would be affected if US surveillance laws were found to lack adequacy. In privacy discussions in the EU, I have heard the view that Section 702 would apply to a narrow set of companies such as Facebook, but not for transfers between the majority of companies. For example, I have heard that companies engaged in normal commerce, such as an international hotel chain, would not be subject to Section 702 directives.

[2] Upon careful research, this narrow proposed interpretation is not consistent with US law. It is true that requests from the US government under Section 702 apply to data collection from "electronic communications service providers." US law defines "electronic communications service provider" broadly, however. US courts have interpreted the relevant definitions to include any company that provides its employees with corporate email or similar ability to send and receive electronic communications. A finding of inadequate protection that applies to Section 702 would thus apply to almost any company with operations in both the EU and US.

I. Text of the Statute

[3] FISA defines the scope of "electronic communications service providers" subject to Section 702 directives at 50 U.S.C. § 1881. Verbatim, the relevant language of the statute reads:

> (b) Additional Definitions
> (4) Electronic Communication Service Provider – The term "electronic communication service provider" means –
> (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
> (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;
> (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;
> (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or
> (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).[1]

II. The Broad Scope of "Electronic Communications Service" under the Electronic Communications Privacy Act

[4] The statute applies if a company falls under any of the subsections (A) through (E).[2] The key subsection is (B) for providers of "electronic communication service" under the Electronic Communications Privacy Act.[3]

[1] 50. U.S.C. § 1881(b)(4).
[2] Note the use of the word "or" under subsection (D).
[3] 18 U.S.C. § 2510.

[5] Subsection (A) and (C) are relatively narrow in scope. With regard to subsection (A), a "telecommunications carrier" is any provider of telecommunications services for a fee as defined by the Communications Act of 1934.[4] This provision covers companies such as AT&T, T-Mobile, and Verizon, as they provide telephone services. Regarding subsection (C), a provider of "remote computing service" refers to "the provision to the public of computer storage or processing," as defined by the Stored Communications Act.[5] This definition would again include AT&T, T-Mobile, and Verizon, because they make computer storage available to the general public (for a fee). It would also include Facebook and Google, as they make computer storage available to the general public (often for free).

[6] Subsection (B) is the legal basis for the expansiveness of the definition of the term "electronic communication service provider" in FISA. Subsection (B) makes any company in-scope if it is considered a provider of "electronic communication service" under the Electronic Communications Protection Act (ECPA). **According to the statutory language in the ECPA, a provider of "electronic communication service" is *any* company that provides users "the ability to send or receive wire or electronic communications."**[6]

[7] The courts have applied this statutory language to employer-provided email. The term "electronic communication service" in the ECPA has been applied to any company that provides electronic communications to its employees, irrespective of the primary function of the business.[7] As one example, Nationwide Insurance Company was found to have provided an electronic communication service because it provided its employees with email services.[8]

[8] The courts' interpretation is confirmed by guidance from the US Department of Justice (DOJ). In its 2009 published guide to obtaining electronic evidence, the DOJ states that any company that provides others with the means to communicate electronically, regardless of their primary business or function, can be a provider of electronic communication service under the ECPA.[9] The guidance says "a mere user of [electronic communication services] provided by another is not a provider of ECS." The guide, however, focuses on whether the entity at issue

---

[4] 47 U.S.C. § 153(44); *see also Virgin Islands Telephone Corp. v. FCC*, 198 F.3d 921 (D.C. Cir. 1999), http://law.justia.com/cases/federal/appellate-courts/F3/198/921/597075/.

[5] 18 U.S.C. § 2711(2). In contrast to the broad scope of "electronic communications service" under the ECPA, the leading interpretation of "remote computing service" is narrower and does not include an internal email system of a company, because it is not made available to the public. *See Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998), https://casetext.com/case/andersen-consulting-llp-v-uop. Other courts have taken a broader view of "remote computing service." *See, e.g., Pure Power Boot Camp v. Warrior Fitness Boot*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008), https://casetext.com/case/pure-power-boot-camp-v-warrior-fitness-boot-camp (ruling that a claim existed against a "remote computing service" regarding emails accessed at work).

[6] 18 U.S.C. § 2510(15). I note that the discussion in this Chapter regards cases that have interpreted the ECPA, not FISA. I am not aware of any reason to believe the use of the term in Section 702 is different. I also am not aware of any declassified FISC opinion that addresses this precise point.

[7] This provision has even been found to apply, for instance, to local governments. In *Bohach v. City of Reno*, the court held that the city fell within the provisions of the ECPA because it provided pager service to its police officers. 932 F. Supp. 1232 (D. Nev. 1996), https://casetext.com/case/bohach-v-city-of-reno.

[8] *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2004), http://openjurist.org/352/f3d/107/fraser-ra-v-nationwide-mutual-insurance-co.

[9] *See* DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 117-18 (2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

provides others with the "means to communicate electronically."[10] It cites the Nationwide case as an example of providing the means to communicate, and cites other included examples such as a business that has a website that offers customers the ability to send messages to third parties.[11]

III. Conclusion

[9] Section 702 and 50 U.S.C § 1881 apply to any "electronic communications service provider." That definition incorporates the definition of any "electronic communications service" under the ECPA, which US courts have interpreted to include any company that provides its employees with corporate email or similar ability to send and receive electronic communications. A finding of inadequate protection based on Section 702 would thus apply to almost any company with operations in both the EU and US.

[10] The EU legal regime as it applies to consent in the employee context means that the broad application of Section 702 may have a particularly strong effect on human resources activities such as internal corporate communications, managing employees, or payroll. Data protection authorities in the EU have been skeptical that individual employees can provide voluntary consent to transfers of their personal data outside of the EU.[12] Furthermore, to the extent consent is valid, it generally remains freely revocable.[13] Companies operating in the EU therefore may face significant challenges in obtaining effective consent from an EU employee to transfer of their personal data to other countries, including the US. Thus, resorting to individual consent as a means of legitimizing transfers in the employment context may not provide effective relief in the face of a finding of inadequacy of protection in the US for Standard Contractual Clauses as a lawful basis for transfer.

---

[10] *Id.* at 117.

[11] *See Becker v. Toca*, 2008 WL 4443050 (E.D. La. Sept. 26, 2008).

[12] The Article 29 Working Party has indicated that when HR data transfers occur as "a necessary and unavoidable consequence of the employment relationship," it would be "misleading" for employers to use consent as a basis because "[i]f it is not possible for the worker to refuse, it is not consent." Thus, "consent will not normally be a way to legitimise [data] processing in the employment context." Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Emp't Context*, 5062/01/EN/Final WP 48 (Sept. 13, 2001) at 3, 23, 28, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

[13] *See id.* at 4 ("[For international transfers,] employers would be ill-advised to rely solely on consent other than in cases where, if consent is subsequently withdrawn, this will not cause problems.").

APPENDIX A:

SOURCE LIST FOR TESTIMONY OF PROFESSOR PETER SWIRE[1]

I. TREATIES AND INTERNATIONAL INSTRUMENTS

Agreement between the European Union and the United States of America on the Protection of Personal Data When Transferred and Processed for the Purpose of Preventing, Investigating, Detecting or Prosecuting Criminal Offences (Draft for Initialing), EU-US, June 2, 2016, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.

Charter of the Fundamental Rights of the European Union. *See* Charter of Fundamental Rights of the European Union, 2000 O.J. C364/01 (Dec. 7, 2000) http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

North Atlantic Treaty, April 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243, http://www.nato.int/cps/en/natohq/official_texts_17120.htm.

Treaty on the Functioning of the European Union, 2012 O.J. C 326/01 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 5, 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

II. EUROPEAN UNION LAW AND GOVERNMENT SOURCES

Regulations, Directives, and Decisions

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, 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

Commission Decision C(2004)5217, Set II: Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers), http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_set_ii_c2004-5721.doc.

Council Decision (EU) No. 2016/920 of 20 May 2016 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, 2016 O.J. (L 154) 1.

[1] Publicly accessible URLs as of November 2, 2016 are provided here and in citations contained in each Chapter.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89, http://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A119%3ATOC&uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG.

European Commission, Annexes to the Commission Implementing Decision 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, C(2016) 4176 final (July 12, 2016), http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf.

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

Case Law, Applications, and Opinions

Zakharov v. Russia, App. No. 47143/06 (Eur. Ct. H.R., Dec. 4, 2015), http://hudoc.echr.coe.int/eng?i=001-159324.

Case C-293/12, *Digital Rights Ireland v. Minister of Commc'ns*, 2014 E.C.R. I-238, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.

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

Case C-362/14, *Schrems v. Data Prot. Comm'r* (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.

Op. of the Advocate General in Joined Cases C-203/15, *Tele2 Sverige AB v. Post-och telestyrelsen* and C-698/15, *Sec. of State for Home Dep't v. Watson* (E.C.J., 2016), http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=EN&mode=req&occ=first.

Other Official Documents, Press Releases, and Online Sources

Article 29 Data Protection Working Party, *Comments of the Working Party to the Vote of 21 October 2013 by the European Parliament's LIBE Committee*, Ref. Ares (2013) 3699166 (Nov. 12, 2013), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131211_annex_letter_to_greek_presidency_wp29_comments_outcome_vote_libe_final_en_.pdf.

Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context*, 5062/01/EN WP 48 (Sept. 2001), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, 16/EN WP 238 (Apr. 13, 2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

Chris Hoofnagle, European Commission Directorate General Justice, Freedom and Democracy, *Commission Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, B.1 – United States of America*, (May 2010), http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b1_usa.pdf.

Committee on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Formal vote on Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of protection provided by the EU-U.S. Privacy Shield, V046420/01, CMTD(2016)0868 (July, 8 2016), http://ec.europa.eu/transparency/regcomitology/index.cfm?do=search.documentdetail&ZMd/3IPPHtzAeedC2zZGx1H1ssUUcBMQ0wtPEeDmiVQXV3U4/r7rgJvJWdYwELHg.

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

Council of Europe Commissioner for Human Rights, *Issue Paper: Democratic and effective oversight of national security services* (2015), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770.

Didier Bigo et al., European Parliament Comm. on Civil Liberties, Justice and Home Affairs, *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law* (2013), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.

European Commission, *Communication from the Commission to the European Parliament and the Council*, COM (2013) 846 (Nov. 27, 2013), http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

European Commission Directorate General for Justice and Consumers, *Guide to the EU-U.S. Privacy Shield* (2016), http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf.

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*, (Apr. 7, 2015), http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e.

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.

European Commission Press Release MEMO16/434, EU-U.S. Privacy Shield: Frequently Asked Questions, (Feb. 29, 2016), http://europa.eu/rapid/press-release_MEMO-16-434_en.htm.

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.

European Commission Proposal for a Council Decision on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, COM (2016) 237 final (Apr. 29, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476055815798&uri=CELEX:52016PC0237.

European Commission, *Rule of Law*, EC.EUROPA.EU, http://ec.europa.eu/justice/effective-justice/rule-of-law/index_en.htm.

European Commission, Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the adoption by Member States of the EU-U.S. Privacy Shield Privacy Shield, Statement 16/2443 (July 8, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm.

European Commission, *The EU-U.S. Privacy Shield*, EC.EUROPA.EU, http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.

European Council, Press Release 305/16, Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign "Umbrella agreement," (June 2, 2016), http://www.consilium.europa.eu/en/press/press-releases/2016/06/02-umbrella-agreement/ (remarks of Dutch Minister Ard van der Steur, who signed the Umbrella Agreement on behalf of the EU).

European Data Protection Supervisor, *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, (May 30, 2016), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf.

European Parliament Comm. on Civil Liberties, Justice and Home Affairs, *Rep. on the US NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, A7-0139/2014 (Feb. 21, 2014), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN.

European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities* (2010), http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf.

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.

Explanations relating to the Charter of Fundamental Rights, 2007 O.J. C303/17, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2007.303.01.0017.01.ENG.

Paul de Hert & Vagelis Papakonstantinou, European Parliament Directorate General for Internal Policies, *The Data Protection Regime in China: In-Depth Analysis for the LIBE Committee*, PE 536.472 EN (Oct. 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

Summary record of the 71st meeting of the Committee on the Protection of Individuals with regard to the Processing of Personal Data (Article 31 Committee), S046419/01 CMTD(2016)0868 (July, 8 2016), http://ec.europa.eu/transparency/regcomitology/index.cfm?do=search.documentdetail&ZMd/3IPPHtzAeedC2zZGx41KHuMFW2Bq3YHOFmINgVoXV3U4/r7rgJvJWdYwELHg.

III. INTERNATIONAL GOVERNMENTAL ORGANIZATIONS

Health Expenditure, Total (% of GDP), THE WORLD BANK, http://data.worldbank.org/indicator/SH.XPD.TOTL.ZS.

IV. IRELAND

Statutes

Criminal Justice (Surveillance) Act 2009 (Act. No. 19/2009) (Ir.), http://www.irishstatutebook.ie/eli/2009/act/19/section/15/enacted/en/html#sec15.

Freedom of Information Act 2014, (Act. No. 30/2014) (Ir.), http://www.irishstatutebook.ie/eli/2014/act/30/enacted/en/html.

Official Secrets Act 1963 (Act. No. 1/1963) (Ir.), http://www.irishstatutebook.ie/eli/1963/act/1/enacted/en/html.

Case Law

Ambiorix Ltd. v. Minister for the Environment [1992] 1 I.R. 277 (S.C.).

Breathnach v. Ireland [1993] 2 IR 458 (H.C.).

Cully v. Northern Bank Finance Corp. [1984] ILRM 683. (H.C.)

McLoughlin v. Aviva Insurance (Europe) Public Ltd. Co. [2011] IESC 42.

Keating v. Radio Telefís Éireann [2013] IEHC 393.

Livingstone v. Minister for Justice [2004] IEHC 58.

Murphy v. Corporation of Dublin [1972] IR 215 (S.C.).

O'Brien v. Ireland [1995] 1 IR 568 (H.C.).

Schrems v. Data Prot. Comm'r [2014] IEHC 310.

Skeffington v. Rooney [1997] 1 IR 22 (S.C.).

Documents Filed with the Court in this Matter

Affidavit of John v. O'Dwyer, *Data Protection Comm'r v. Facebook Ireland Ltd.*, No. 2016/4809P (filed July 4, 2016) (H.C.).

Plaintiff's Reply to the Defence of the First Named Defendant, *Data Protection Comm'r v. Facebook Ireland Ltd.*, No. 2016/4809P (filed Sept. 30, 2016) (H.C.).

Draft Decision of the Data Protection Comm'r, *Schrems v. Facebook Ireland Ltd.*, No. 3/15/766 (May 24, 2016).

Other

CENTRAL STATISTICS OFFICE, PROFILE 1 TOWN AND COUNTRY (Apr. 2012) (Ir.), http://www.cso.ie/en/media/csoie/census/documents/census2011vol1andprofile1/Profile1_Town_and_Country_Entire_doc.pdf.

V. UNITED STATES LAW AND GOVERNMENT SOURCES

Constitutions

Federal

U.S. CONST. arts. I, III, V.

U.S. CONST. amends. I, III, IV, V, VI, VII, VIII, XI, XVI, XXIV.

State

ALASKA CONST. art. I, § 22.

CAL. CONST. art. I, § 1.

FLA. CONST. art. I, § 23.

MONT. CONST. art. II, § 10.

Statutes[2]

Federal

Administrative Procedure Act (APA), 5 U.S.C. §§ 551-559.

Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-06.

Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3 §§ 1-16.

Communications Act of 1934, 47 U.S.C. §§ 151-62.

Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001-10.

[2] Statutes are listed by name where named and by section where unnamed.

Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. §§ 7701-13.

Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), Pub. L. No. 111-203, 1055(a)(2)(G), 124 Stat. 1376 (codified in scattered sections of 5 U.S.C. App, 7 U.S.C, 12 U.S.C., and 15 U.S.C.).

Driver's Privacy Protection Act of 1994 (DPPA), Title XX of the Violent Crime Control and Law Enforcement Act, 18 U.S.C. §§ 2721-25.

Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. 99–508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

Electronic Funds Transfer Act (EFTA), Pub. L. 95-630, 92 Stat. 3641 (codified in scattered sections of 12 U.S.C. and 15 U.S.C.).

Espionage Act of 1917, Pub. L. 65-24, 40 Stat. 217 (codified at 18 U.S.C. §§ 791-799).

Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681-1681x.

Fair Debt Collection Practices Act (FDCPA), 15 U.S.C. §§ 1692-1692p.

Federal Trade Commision Act of 1914 (FTC Act), 15 U.S.C. § 41-77.

Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. 95–511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261 (codified in scattered sections of 50 U.S.C.).

Freedom of Information Act (FOIA), 5 U.S.C. § 552.

Gramm-Leach-Bliley Act (GLBA), Pub. L. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 U.S.C. and 15 U.S.C.).

Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), Pub. L. 111-5, 123 Stat. 115, Title XIII (codified in scattereds ections of 42 U.S.C.).

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (codified in scattered sections of 29 U.S.C., and 42 U.S.C.).

Intelligence Community Whistleblower Protection Act of 1998 (ICWPA), 50 U.S.C. § 403q.

Inspector General Act of 1978, 5 U.S.C. App. 1 §§ 1-13.

Intelligence Reform and Terrorism Prevention Act of 2004, 42 U.S.C. § 2000ee.

Judicial Redress Act of 2015, 5 U.S.C. § 552a.

Privacy Act of 1974, 5 U.S.C. § 552a.

Protect America Act, 50 U.S.C. §§ 1801-13.

Right to Financial Privacy Act of 1978 (RFPA), 12 U.S.C. §§ 3401-22.

Securities Act of 1933, 15 U.S.C. §§ 77a-77aa.

Stored Communications Act (SCA), 18 U.S.C. §§ 2701–12.

Telecommunications Act of 1996, 47 U.S.C. §§ 101-622.

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. No. 114-23, H.R. 2048, (codifed in scattered sections of 12 U.S.C., 15 U.S.C., 18 U.S.C., and 50 U.S.C.).

Uniting and Strengthening America by Providing the Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), Pub. L. 107-56 (2001), 115 Stat. 272.

USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 115 Stat. 272 (codified as amended in scattered sections of 8 U.S.C., 12 U.S.C., 15 U.S.C., 18 U.S.C., 20 U.S.C., 31 U.S.C., 42 U.S.C., 47 U.S.C., 49 U.S.C., 50 U.S.C.).

Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710.

Wiretap Act, 18 U.S.C. §§ 2510-21.

42 U.S.C. § 1983.

State

18 PA. CONS. STAT. § 4107(a)(10).

ALA. CODE § 8-35-1.

CAL. CIV. CODE §§ 1785.10-19.5, 1798.29, 1798.80-98.4.

California Computer Misuse and Abuse Act (CMAA), CAL. PENAL CODE §§ 484-502.9.

California Confidentiality of Medical Information Act (CMIA), CAL. CIV. CODE §§ 56-56.37.

California Consumer Credit Reporting Agencies Act (CCRAA), CAL. CIV. CODE §§ 1785.1-.6.

California Consumers Legal Remedies Act (CLRA), CAL. CIV. CODE §§ 1750-84.

California Electronic Communications Privacy Act (CalECPA), CAL. PENAL CODE §§ 1546-1546.4.

California Financial Information Privacy Act (FIPA), CAL. FIN. CODE §§ 4050-60.

California Invasion of Privacy Act (CalCIPA), CAL. PENAL CODE § 630-638-55.

California Online Privacy Protection Act (CalOPPA), CAL. BUS. & PROF. CODE §§ 22575-79.

California Spam Laws, CAL. BUS. & PROF. CODE §§ 17529, 17538.45.

California Unfair Competition Law (UCL), CAL. BUS. & PROF. CODE §§ 17200-210.

CONN. GEN. STAT. § 42-471.

Delaware Online Privacy and Protection Act, DEL. CODE ANN. tit. 6, § 1205C.

ILL. COMP. STAT., §505/2MM

Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. 505-1-505/12.

IND. CODE §§ 24-5-24, 24-5-24.5.

KY. REV. STAT. ANN. §§ 367.363-.370.

MASS. GEN. LAWS ch. 214, § 1.

MINN. STAT. §§ 325M.01-.09.

NEB. REV. STAT. § 87-302.

NEV. REV. STAT. § 205.498.

WASH. REV. CODE § 19.182.170 *et seq.*

Washington Fair Credit Reporting Act, 19 WASH. REV. CODE §§ 182.005-.902.

Regulations

16 C.F.R. § 681.2(c).

17 C.F.R. § 248.

45 C.F.R. § 160.

47 C.F.R. § 42.6.

Rules

FED. R. CRIM. P. 16, 29.

FED. R. EVID. 103.

FED. R. CIV. P. 23.

F.I.S.C. R.P. 5-8, 11, 13, 17, 22, 62.

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.

Executive Orders and Presidential Directives

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.

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.

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.

Case Law – Opinions and Orders

Federal

Am. C.L. Union v. Clapper, 785 F.3d 787, 801 (2d Cir. 2015).

Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190 (9th Cir. 2007).

Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998).

Bareford v. Gen. Dynamics Corp., 973 F.2d 1138 (5th Cir. 1992).

Bartnicki v. Vopper, 532 U.S. 514 (2001).

Batmanghelich v. Sirius XM Radio Inc., No. 2:09-cv-09190 (C.D. Cal. 2011) (not reported).

Becker v. Toca, No. Civ. A. 07-7202 (E.D. La. 2008) (not reported).

Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971).

Breedlove v. Suttles, 302 U.S. 277 (1937).

Brinegar v. United States, 338 U.S. 160 (1949).

Brown v. Defender Sec. Co., 2:12-cv-07319-CAS (PJW) (C.D. Cal. 2013) (not reported).

[Caption Redacted], No. PR/TT [Redacted] (F.I.S.C. June 22, 2009).

[Caption Redacted], No. PR/TT [Redacted] (F.I.S.C. [Date Redacted]).

[Caption Redacted], No. PR/TT [Redacted] (F.I.S.C. [month & day redacted], 2004).

[Caption Redacted], No. [Redacted], 2011 WL 10945618 (F.I.S.C. Oct.3, 2011).

[Caption Redacted], No. [Redacted], 2011 WL 10947772 (F.I.S.C. Nov. 30, 2011).

[Caption Redacted], No. [Redacted] (F.I.S.C. Aug. 26, 2014).

[Caption Redacted], No. [Redacted] (F.I.S.C. Nov. 6, 2015).

[Caption Redacted], No. [Redacted] (F.I.S.C. Sept. 25, 2012).

Chisholm v. Georgia, 2 U.S. 419 (1793).

CIA v. Sims, 471 U.S. 159 (1985).

Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013).

Cohorst v. BRE Props., No. 3:10-cv-2666-JM-BGS (S.D. Cal. 2011) (not reported).

Coulter-Owens v. Rodale, Inc., No. 2:14-cv-12688 (E.D. Mich. 2016) (not reported).

Curry v. AvMed, Inc., No. 1:10-cv-24513-JLK (S.D. Fla. 2013) (not reported).

Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

Doe v. Gonzales, 386 F. Supp. 2d 66 (D. Conn. 2005).

Ellsberg v. Mitchell, 709 F.2d 51 (D.C. Cir. 1983).

Fraley v. Facebook, Inc., 830 F. Supp. 2d 785 (N.D. Cal. 2011).

Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003).

Fort Hall Landowners Alliance, Inc. v. Department of Interior, No. 4:99-cv-00052-BLW (D. Idaho 2007) (not reported).

FTC v. AT&T Mobility LLC, No. 15-16585 (9th Cir. 2016) (not reported).

Galaria v. Nationwide Mut. Ins. Co., No. 15-3386, 2016 WL 4728027 (6th Cir. Sept. 12, 2016).

Gen. Dynamics Corp. v. United States, 563 U.S. 478 (2011).

Graham v. Richardson, 403 U.S. 365 (1971).

Harris v. ComScore, Inc., No. 11-cv-5807 (N.D. Ill. 2014) (not reported).

Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994).

Holland v. Yahoo! Inc., No. 5:13-cv-4980 (N.D. Cal. 2016) (not reported).

Horton v. California, 496 U.S. 128 (1990).

In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 995 (N.D. Cal. 2016).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 15-75, Misc. No. 15-01, 2015 WL 5637562 (F.I.S.C. June 29, 2015).

In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 09-13, 2009 WL 9150914 (F.I.S.C. Sept. 3, 2009).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 09-13, 2009 WL 9150896 (F.I.S.C. Sept. 25, 2009).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things [Redacted], No. BR 13-109 (F.I.S.C. Aug. 23, 2013).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things [Redacted], No. BR 13-109, 2013 WL 5741573 (F.I.S.C. Aug. 29, 2013).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 13-109 (F.I.S.C. Sept. 17, 2013).

In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-158 at 6 (F.I.S.C. Oct. 11, 2013).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things [Redacted], No. BR 13-158 (F.I.S.C. Oct. 15, 2013).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 13-158 (F.I.S.C. Oct. 18, 2013).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 14-96, 2014 WL 5463290 at 12 (F.I.S.C. June 19, 2014).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 14-96 (F.I.S.C. June 26, 2014).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 14-01, 2014 WL 5463107 (F.I.S.C. Apr. 11, 2014).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 14-01, 2014 WL 5463097 (F.I.S.C. Mar. 20, 2014).

In re Application of the F.B.I. for an Order Requiring the Production of Tangible Things, No. BR 14-01 (F.I.S.C. Mar. 21, 2014).

In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 14-01 at 2 (F.I.S.C. Apr. 11, 2014).

In re AT&T Servs., Inc., FCC Rcd. DA 15-399 (2015).

In re Black iPhone 4, 27 F. Supp. 3d 74 (D.D.C. 2014).

In re Barnes & Noble Pin Pad Litig., No. 12-CV-08617, 2016 WL 5720370 (N.D. Ill. Oct. 3, 2016).

In re Carrier iQ, Inc. Consumer Privacy Litig., No. 3:12-md-02330-EMC (N.D. Cal. 2016) (not reported).

In re Cellco P'ship, d/b/a Verizon Wireless, FCC Rcd. DA 16-242 (2016).

In re Certified Question of Law, No. FISCR 16-01 (F.I.S.C.R. Apr. 14, 2016).

In [Redacted] a U.S. Person, No. PR/TT 2016-[Redacted] (F.I.S.C. Feb. 12, 2016).

In re Dep't of Veterans Affairs (VA) Data Theft Litig., MDL No. 1796 (D.D.C. 2009) (not reported).

In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act, No. 105B(G): 07-01 at 2 (F.I.S.C. Dec. 28, 2007).

In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act, No. 105B(G): 07-01 (F.I.S.C. Feb. 6, 2008).

In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act, No. 105B(G): 07-01 at 3-4, 43 (F.I.S.C. Apr. 25, 2008).

In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act, No. 105B(G): 07-01 at 1 (F.I.S.C. Jan. 4, 2008).

In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act, No. 105B(G): 07-01 (F.I.S.C.R. Aug. 22, 2008).

In re DNI/AG Certification [Redacted], No. 702(i)-08-01 (F.I.S.C. Sept. 4, 2008).

In re EasySaver Rewards Litig., 921 F. Supp. 2d 1040 (S.D. Cal. 2013).

In re Google Buzz User Privacy Litig., No. 5:10-cv-00672-JW (N.D. Cal. 2010) (not reported).

In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (11th Cir. 2012).

In re Morgan Stanley Smith Barney LLC, SEC File No. 3-17280, Release No. 78012 (2016).

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. 2013).

In re Motion for Declaratory Judgment that LinkedIn Corp. May Report Aggregate Data Regarding FISA Orders, No. 13-07 (F.I.S.C. 2013).

In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders & Directives, No. Misc. 13-06 (F.I.S.C. 2013).

In re Motion to Disclose Aggregate Data Regarding FISA Orders, No. Misc. 13-05 (F.I.S.C. 2013).

In re Motion to Disclose Aggregate Data Regarding FISA Orders, No. Misc. 13-04 (F.I.S.C. 2013).

In re Motion to Disclose Aggregate Data Regarding FISA Orders, No. Misc. 13-03 (F.I.S.C. 2013).

In re Netflix Privacy Litig., 5:11-CV-00379 EJD (N.D. Cal. 2013) (not reported).

In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act, No. Misc. 13-02 (F.I.S.C. Sept. 13, 2013).

In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act, No. Misc. 13-02, -03, -04 (F.I.S.C. July 18, 2013)

In re Orders of this Court Interpreting Section 215 of the Patriot Act, No. Misc. 13-02, 2014 WL 5442058 (F.I.S.C. Aug. 7, 2014).

In re Orders of this Court Interpreting Section 215 of the Patriot Act, No. Misc. 13-02 (F.I.S.C. Nov. 20, 2013).

In re Production of Tangible Things from [Redacted], No. BR 08-13, 2009 WL 9157881 (F.I.S.C. Jan. 28, 2009).

In re Production of Tangible Things from [Redacted], No. BR 08-13 (F.I.S.C. Mar. 2, 2009).

In re Quantcast Advert. Cookie Litig., No. 2:10-cv-05484 (C.D. Cal. 2010) (not reported).

In re [Redacted], No. [Redacted] (F.I.S.C. Apr. 3, 2007).

In re Sealed Case, 310 F.3d 717 (F.I.S.C. 2002).

In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014).

In re TerraCom, Inc., & YourTel Am., Inc., FCC Rcd. DA 15-776 (2015).

In re Trans Union Corp. Privacy Litig., 741 F.3d 811 (7th Cir. 2014).

In re Trans Union Corp. Privacy Litig., No. 1:00-cv-04729 (N.D. Ill. 2008) (not reported).

In re Verizon Compliance with the Comm'n's Rules & Regulations Governing Customer Proprietary Network Info., FCC Rcd. DA 14-1251 (2014).

In re Webloyalty.com, Inc., Mktg. & Sales Practices Litig., No. 1:07-MD-018-JLT (D. Mass. 2009) (not reported).

Jewel v. Nat'l Sec. Agency, No. 07-cv-00693-JSW (N.D. Cal. 2015) (not reported).

Kasza v. Browner, 133 F.3d 1159 (9th Cir. 1998).

Kehoe v. Fidelity Fed. Bank & Trust, No. 03-80593-CIV-Hurley/Lynch (S.D. Fla. 2006) (not reported).

Kinder v. Meredith Corp., No. 1:14-cv-11284 (E.D. Mich. 2016) (not reported).

Klayman v. Obama, 142 F. Supp. 3d 172, 186 (D.D.C. 2015).

Lane v. Facebook, Inc., No. 08-cv-3845 RS (N.D. Cal. 2010) (not reported).

Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016).

Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992).

Mapp v. Ohio, 367 U.S. 643 (1961).

Marenco v. Visa, Inc., 2:10-cv-08022 (C.D. Cal. 2011) (not reported).

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

Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016).

Minnesota v. Accretive Health, Inc., No. 0:12-cv-00145 (D. Minn. 2012) (not reported).

Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014).

[Name Redacted], No. PR/TT [Redacted] and Previous Dockets (F.I.S.C. [date redacted]).

New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

New York Times Co. v. United States, 403 U.S. 713 (1971).

Order on Motion of Apple, Inc. for Leave to File Amicus Curiae Brief, *In re Motions to Disclose Aggregate Data Regarding FISA Orders and Directives*, 13-03; 13-04; 13-05; 13-06; 13-07 (F.I.S.C. Nov. 13, 2013).

Order on Mot. of DropBox, Inc. for Leave to File Amicus Curiae Brief, *In re Motions to Disclose Aggregate Data Regarding FISA Orders and Directives*, No.s 13-03; 13-04; 13-05; 13-06; 13-07 (F.I.S.C. filed Oct. 1, 2013).

Perkins v. LinkedIn Corp., CNo. 5:13-cv-04303-LHK (N.D. Cal. 2015) (not reported).

Peterson v. Lowe's HIW, Inc., No. 3:11-cv-01996-RS (N.D. Cal. 2012) (not reported).

Plyler v. Doe, 457 U.S. 202 (1982).

Pollock v. Farmers' Loan & Trust Co., 157 U.S. 429 (1895).

Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

Preliminary Notice of a Potential Compliance Incident Involving [Redacted], (F.I.S.C. filed [date redacted]).

Reed v. 1-800 Contacts, Inc., MDL No. 12-2359f (S.D. Cal. 2014) (not reported).

Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015).

Shearson v. Holder, 725 F.3d 588, 593 (6th Cir. 2013).

Smith v. Maryland, 442 S.S. 735 (1979).

Stone v. Howard Johnson Int'l, Inc., No. 2:12-cv-01684 (C.D. Cal. 2015) (not reported).

Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726 (9th Cir. 2011).

Terry v. Ohio, 392 U.S. 1 (1968).

United States v. Ali, 870 F. Supp. 2d 10 (D.D.C. 2012).

United States v. Anderson, 872 F.2d 1508 (11th Cir. 1989).

United States v. Ganias, 755 F.3d 125 (2d Cir. 2014).

United States v. Google Inc., No. 3:12-cv-04177-SI (N.D. Cal. 2012) (not reported).

United States v. Morton Salt Co., 338 U.S. 632 (1950).

United States v. O'Hara, 301 F.3d 563 (7th Cir. 2002).

United States v. Path, Inc., No. 3:13-cv-00448-RS (N.D. Cal. 2013) (not reported)

United States v. Reynolds, 345 U.S. 1 (1953).

United States v. Rivera, 527 F.3d 891 (9th Cir. 2008).

United States v. Sony BMG Music Entm't, No. 08-civ-10730-LAK (S.D.N.Y. 2008) (not reported).

United States v. U.S. Dist. Court for E. Dist. of Mich., 407 U.S. 297 (1972).

United States v. Verdugo-Urquidez, 494 U.S. 1092 (1990).

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

United States v. Xanga.com, Inc., No. 06-cv-6853-SHS (S.D.N.Y. Sept. 12, 2006) (not reported).

United States v. Yunis, 867 F.2d 617 (D.C. Cir. 1989).

Virgin Islands Tel. Corp. v. FCC, 198 F.3d 921 (D.C. Cir. 1999).

Weinberger v. Catholic Action of Hawaii/Peace Educ. Project, 454 U.S. 139 (1981).

Wong Sun v. United States, 371 U.S. 471 (1963).

Yang v. Reno, 157 F.R.D. 625 (M.D. Pa. 1994).

Young v. Hilton Worldwide, Inc., 565 Fed. App'x 595 (9th Cir. 2014).

Zuckerbraun v. Gen. Dynamics Corp., 935 F.2d 544 (2d Cir. 1991).

State

Mount v. Wells Fargo Bank, N.A., No. B260585 (Cal. App. Ct. 2016) (not reported).

Saunders v. StubHub Inc., No. CGC-12-517707 (Cal. App. Dep't Super. Ct. 2015) (not reported).

Snow v. LensCrafters, Inc., No. CGC-02-405544 (Cal. App. Dep't Super. Ct. 2008) (not reported).

Tien v. Superior Court, 139 Cal. App. 4th 528 (Cal. Ct. App. 2006).

Utility Consumers' Action Network v. Bank of Am., N.A., No. CJC-01-004211 (Cal. App. Dep't Super. Ct. 2007) (not reported).

Case Law – Motions, Briefs, and Other Court Documents

Brief of *Amici Curiae* [Media Companies], *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, *In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders & Directives*, No. Misc. 13-04, *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. 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Brief-3.pdf.

Brief of *Amici Curiae* [Congressional Representatives], *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (F.I.S.C. 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Brief-1.pdf.

Brief of Appellant Yahoo!, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed May 29, 2008), https://www.dni.gov/files/documents/0909/Yahoo%20Brief%2020080529.pdf.

Declassified Certification of Attorney General Michael B. Mukasey, *In re Nat'l Sec. Agency Telecommunications Records Litig.*, MDL No. 06-1791-VRW (N.D. Cal. Sept. 19, 2008), http://www.dni.gov/files/documents/0505/AG%20Mukasey%202008%20Declassified%20Declaration.pdf.

Ex-Parte Brief for Respondent, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed June 5, 2008), https://www.dni.gov/files/documents/0909/Government%20Ex%20Parte%2020080605.pdf.

Ex-Parte Supplemental Brief for Respondent, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed June 26, 2008), https://www.dni.gov/files/documents/0909/Government%20Supplemental%20Brief%2020080626.pdf.

Facebook's Mot. For Declaratory Judgment, *In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives*, No. Misc. 13-06 (F.I.S.C. filed Sept. 9, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-06%20Motion-3.pdf

FISC Docket 105B(g) 07-01, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, https://www.dni.gov/files/documents/0909/Docket%20Entry%20Sheet.pdf.

Government's Mot. to Compel, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Nov. 21, 2007), https://www.dni.gov/files/documents/0909/Government%20Motion%2020071121.pdf.

Government's Mot. to Compel, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Nov. 30, 2007), https://www.dni.gov/files/documents/0909/Yahoo%20Opposition%20Memo%2020071130.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.

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.

Mot. for Declaratory Judgment that LinkedIn Corporation May Report Aggregate Data Regarding FISA Orders, *In re Motion for Declaratory Judgment that LinkedIn Corp. May Report Aggregate Data Regarding FISA Orders*, No. 13-07 (F.I.S.C. filed Sept. 17, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-07%20Motion-3.pdf.

Mot. for Leave to File a Supplementary Reply Brief, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (filed July 3, 2008), https://www.dni.gov/files/documents/0909/Government%20Motion%2020080703.pdf.

Mot. for Leave to File Reply to the Government's Supplemental Briefing *Instanter, In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (filed June 30, 2008), https://www.dni.gov/files/documents/0909/Yahoo%20Motion%2020080630.pdf.

Mot. of the ACLU et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, 2014 WL 5442058 (F.I.S.C. Sep. 13, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-1.pdf.

Mot. of the Reporters Committee for Freedom of the Press et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, -03, -04 (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-4.pdf;

Mot. of US Representatives Amash et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-2.pdf.

Mot. of the First Amendment Coal. et al. for Leave to file Brief as *Amici Curiae*, in Support of the Motions for Declaratory Judgment, *In re Motion for Declaratory Judgment of Google, Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, No. Misc. 13-03, 13-04; (F.I.S.C. filed July 8, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-12.pdf.

Preliminary Notice of a Potential Compliance Incident Involving [Redacted], (F.I.S.C. filed [date redacted]), https://www.dni.gov/files/0808/Final%20037.Preliminary%20Notice%20of%20Potential%20Compliance%20Incident.pdf.

Reply Brief of Appellant Yahoo! *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed June 9, 2008), http://www.documentcloud.org/documents/1300533-3-yahoo-reply-brief.html.

Rep. of the United States, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 09-09 (F.I.S.C. filed Aug. 17, 2009), https://www.dni.gov/files/documents/section/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf

Transcript of June 19, 2008 Oral Argument, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. June 19, 2008), https://www.dni.gov/files/documents/1118/19%20June%202008%20FISCR%20PAA%20Hearing%20Transcript%20-%20Declassified%20FINAL.pdf.

Yahoo!'s Mot. for Declaratory Judgement [sic] to Disclose Aggregate Data Regarding FISA Orders and Directives, *In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives*, No. Misc. 13-05 (F.I.S.C. filed Sept. 9, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-05%20Motion-12.pdf

Government Reports

CHARLES DOYLE, CONG. RESEARCH SERV., RL 32186, USA PATRIOT ACT SUNSET: PROVISIONS THAT EXPIRE ON DECEMBER 31, 2005 (June 29, 2005) http://www.fas.org/sgp/crs/intel/index.html.

DEP'T OF HOMELAND SEC. OFFICE OF INSPECTOR GEN., 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.

DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL § 2054, https://www.justice.gov/usam/criminal-resource-manual-2054-synopsis-classified-information-procedures-act-cipa.

DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (March 2008), https://oig.justice.gov/special/s0803b/final.pdf.

DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS (Jan. 2010), https://oig.justice.gov/special/s1001r.pdf.

DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (March 2007), https://oig.justice.gov/special/s0703b/final.pdf.

DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF PROGRESS IN IMPLEMENTING RECOMMENDATIONS AND EXAMINATION OF USE IN 2007 AND 2009 (Aug. 2014), https://oig.justice.gov/reports/2014/s1408.pdf.

DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

JOHN ROTH, DEP'T OF HOMELAND SEC. OFFICE OF INSPECTOR GEN., INVESTIGATION INTO THE IMPROPER ACCESS AND DISTRIBUTION OF INFORMATION CONTAINED WITHIN A SECRET SERVICE DATA SYSTEM (Sept. 25, 2015), https://www.oig.dhs.gov/assets/Mga/OIG_mga-092515.pdf.

NSA CIVIL LIBERTIES AND PRIVACY OFFICE, TRANSPARENCY REPORT: THE USA FREEDOM ACT BUSINESS RECORDS FISA IMPLEMENTATION (Jan. 15, 2016), https://www.nsa.gov/about/civil-liberties/reports/assets/files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

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/assets/files/nsa_clpo_report_targeted_EO12333.pdf.

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/assets/files/nsa_report_on_section_702_program.pdf.

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.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR JUNE 1, 2012 TO NOVEMBER 30, 2012 (2013), https://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR JUNE 1, 2009 TO NOVEMBER 30, 2009 (2010), http://www.dni.gov/files/documents/FAA/SAR%20May%202010%20Final%20Release%20with%20Exemptions.pdf.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR DECEMBER 1, 2008 TO MAY 31, 2009 (2010), http://www.dni.gov/files/documents/FAA/SAR%20December%202009%20Final%20Release%20with%20Exemptions.pdf.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR SEPTEMBER 4, 2008 TO NOVEMBER 30, 2008 (2009), http://www.dni.gov/files/documents/FAA/SAR%20March%202009%20Final%20Release%20with%20Exemptions.pdf

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CIA 2015 MINIMIZATION PROCEDURES (July 15, 2015), https://www.dni.gov/files/documents/2015CIAMinimizationProcedures_Redacted.pdf.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CIVIL LIBERTIES AND PRIVACY OFFICE, CIVIL LIBERTIES AND PRIVACY INFORMATION PAPER: DESCRIPTION OF CIVIL LIBERTIES AND PRIVACY PROTECTIONS INCORPORATED IN THE 2008 REVISION OF EXECUTIVE ORDER 12333 (2008, and revised in 2013) https://www.dni.gov/files/documents/CLPO/CLPO_Information_Paper_on_2008_Revision_to_EO_12333.pdf.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Declassified: Release of FISC Question of Law and FISCR Opinion*, IC ON THE RECORD (Aug. 22, 2016), https://icontherecord.tumblr.com/tagged/declassified .

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, MINIMIZATION PROCEDURES USED BY THE NSA IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (July 15, 2015), https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf.

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.

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 (July 2014), https://fas.org/irp/dni/ppd28-status.pdf.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform, 2015 Anniversary Report – Enhancing Transparency*, IC ON THE RECORD (2015), https://icontherecord.tumblr.com/ppd-28/2015/enhancing-transparency.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform 2015 Anniversary Report – Limiting SIGINT Collection and Use*, IC ON THE RECORD (2015), http://icontherecord.tumblr.com/ppd-28/2015/limiting-sigint-collection.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Signals Intelligence Reform 2015 Anniversary Report – Strengthening Privacy and Civil Liberties Protections*, IC ON THE RECORD (2015), http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#section-215.

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.

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.

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.

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.

OFFICE OF THE INSPECTOR GEN. OF THE INTELLIGENCE COMMUNITY, OCTOBER 1, 2015 – MARCH 31, 2016 SEMIANNUAL REPORT TO THE DIRECTOR OF NATIONAL INTELLIGENCE (2016), https://www.dni.gov/files/documents/ICIG/ICIG-SAR-UNCLASS-OCT15-MAR16.pdf.

PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY (Dec. 12, 2014), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, RECOMMENDATIONS ASSESSMENT REPORT, (Jan. 29, 2015), https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf.

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

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.

REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE US COURTS ON ACTIVITIES OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS FOR 2015, http://www.uscourts.gov/statistics-reports/analysis-reports/directors-report-foreign-intelligence-surveillance-courts.

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.

Official Documents, Press Releases, and Other Sources

Federal

CENT. INTELLIGENCE AGENCY, SIGNALS INTELLIGENCE ACTIVITIES (undated), https://www.dni.gov/files/documents/ppd-28/CIA.pdf.

DEP'T OF JUSTICE, *Fact Sheet: Department of Justice Corrective Actions on FBI's Use of National Security Letters* (Mar. 20, 2007), https://www.justice.gov/archive/opa/pr/2007/March/07_nsd_168.html.

DEP'T OF JUSTICE, *Office of Intelligence* (July 23, 2014), https://www.justice.gov/nsd/office-intelligence.

DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GEN., Letters dated Apr. 28, 2016 from Peter J. Kadzik, Assistant Attorney Gen. regarding Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2015 1-2 (2016), https://www.justice.gov/nsd/nsd-foia-library/2015fisa/download.

DEP'T OF JUSTICE, *Sections & Offices*, at "Oversight Section," https://www.justice.gov/nsd/sections-offices#oversight.

ECPA (Part 1): Lawful Access to Stored Content: Hearing before the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary, 113th Cong. 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Attorney Gen., Office of Legal Policy, Dep't of Justice), https://judiciary.house.gov/_files/hearings/printers/113th/113-16_80065.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.

FEDERAL TRADE COMMISSION, *About the FTC*, https://www.ftc.gov/about-ftc.

FEDERAL TRADE COMMISSION, *Cases and Proceedings*, https://www.ftc.gov/enforcement/cases-proceedings.

FEDERAL COMMUNICATIONS COMMISSION, *Fact Sheet: Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice over their Personal Information* (Oct. 6, 2016), https://www.fcc.gov/document/fact-sheet-broadband-consumer-privacy-proposal.

FEDERAL COMMUNICATIONS COMMISSION, *What We Do*, https://www.fcc.gov/about-fcc/what-we-do.

Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy Before the S. Comm. on the Judiciary, 114th Cong. (2015) (statement of Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business Georgia Institute of Technology), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf.

Joint Unclassified Statement to the H. Comm. on the Judiciary, 114th Cong. (2016) (statement of Robert Litt, General Counsel of the Office of the Dir. of Nat'l Intelligence, et al.), https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2016/02/17/508_compliant_02-02-16_fbi_litt_evans_steinbach_darby_joint_testimony_from_february_2_2016_hearing_re_fisa_amendments_act.pdf.

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.

Letter dated July 7, 2016 from Edith Ramirez, Chairwoman, Federal Trade Commission, to Věra Jourová, Comm'r for Justice, Consumers and Gender Equality, European Commission, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0v.

Letter dated Oct. 11, 2013 from Reggie B. Walton, FISC Chief Judge, to Patrick J. Leahy, Chairman of the US Senate Judiciary Committee, https://fas.org/irp/agency/doj/fisa/fisc-101113.pdf.

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.

NATIONAL SECURITY AGENCY, *Civil Liberties and Privacy Home* (May 3, 2016), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *About the Review Group on Intelligence and Communications Technologies*, https://www.dni.gov/index.php/intelligence-community/review-group.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *IC Inspector General*, DNI.GOV, https://www.dni.gov/index.php/about/leadership/inspector-general#.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, IC ON THE RECORD, http://icontherecord.tumblr.com.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *IC on the Record Posts Tagged "Becky Richards,"* IC ON THE RECORD, http://icontherecord.tumblr.com/tagged/becky+richards.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *IC on the Record Statement Accompanying Posting of EO 12333 Table of Guidelines*, IC ON THE RECORD (July 20, 2016), https://icontherecord.tumblr.com/post/147708188298/ic-on-the-record-statement-accompanying-posting-of.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Inspector General of the Intelligence Community: Who We Are*, DNI.GOV, https://www.dni.gov/index.php/about/organization/office-of-the-intelligence-community-inspector-general-who-we-are.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, OFFICE OF CIVIL LIBERTIES, PRIVACY AND INTELLIGENCE, *Who We Are*, https://www.dni.gov/index.php/about/organization/civil-liberties-privacy-office-who-we-are.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Principles of Intelligence Transparency for the Intelligence Community*, http://www.dni.gov/files/documents/ppd-28/FINAL%20Transparency_poster%20v1.pdf.

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.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Oversight: Release of Joint Assessments of Section 702 Compliance*, IC ON THE RECORD (July 21, 2016), https://icontherecord.tumblr.com/post/147761829243/release-of-joint-assessments-of-section-702.

OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statement by the Office of the Director of National Intelligence and the Department of Justice on the Declassification of Documents Related to Section 702 of the Foreign Intelligence Surveillance Act*, IC ON THE RECORD (Sept. 29, 2015), https://icontherecord.tumblr.com/post/130138039058/statement-by-the-office-of-the-director-of.

Peter Swire, Testimony before the US Senate Commerce Comm. on "How Will the 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.

Peter Swire, Testimony before the Senate Judiciary Comm., Subcomm. on the Constitution, "Responding to the Inspector General's Findings of Improper Use of National Security Letters by the FBI," (Apr. 11, 2007) https://www.judiciary.senate.gov/imo/media/doc/swire_testimony_04_11_07.pdf.

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.

Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire (Sept. 16, 1999), WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, http://intellit.muskingum.edu/cryptography_folder/encryption2.htm.

Press Release, Federal Bureau of Investigation, Response to DOJ Inspector General's Report on FBI's Use of National Security Letters, https://archives.fbi.gov/archives/news/pressrel/press-releases/response-to-doj-inspector-general2019s-report-on-fbi2019s-use-of-national-security-letters.

Press Release, Federal Communications Comm'n, FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency, and Security for their Personal Data (Oct. 27, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1027/DOC-341937A1.pdf.

Press Release, Securities and Exchange Comm'n, Morgan Stanley Failed to Safeguard Customer Data (June 8, 2016), https://www.sec.gov/news/pressrelease/2016-112.html.

Press Release, Securities and Exchange Comm'n, SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to the Breach (Sept. 22, 2015), https://www.sec.gov/news/pressrelease/2015-202.html.

Press Release, US Dep't of Health and Human Services, Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University (July 18, 2016), http://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html.

Press Release, Office of the Director of National Intelligence and the Department of Justice, Statement by the ODNI and the U.S. DOJ on the Declassification of Documents Related to the Protect American Act Litigation (Sept. 11, 2014), https://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1109-statement-by-the-office-of-the-director-of-national-intelligence-and-the-u-s-department-of-justice-on-the-declassification-of-documents-related-to-the-protect-america-act-litigation.

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.

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *Board Members*, https://pclob.gov/about-us/board.html.

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, PCLOB.GOV, https://pclob.gov/.

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *What is the Privacy and Civil Liberties Oversight Board?* https://www.pclob.gov/.

Tom Wheeler, *Protecting Privacy for Broadband Consumers*, FEDERAL COMMUNICATIONS COMMISSION (Oct. 6, 2016), https://www.fcc.gov/news-events/blog/2016/10/06/protecting-privacy-broadband-consumers.

SECURITIES AND EXCHANGE COMM'N, *About the SEC*, https://www.sec.gov/about.shtml.

US CENSUS BUREAU, *California QuickFacts*, http://www.census.gov/quickfacts/table/PST045215/06.

US DEP'T OF COMMERCE, PRIVACY SHIELD FRAMEWORK (2016), https://www.privacyshield.gov/welcome.

US DEP'T OF COMMERCE, PRIVACY SHIELD FRAMEWORK, *Access Requests by Public Authorities* (2016), https://www.privacyshield.gov/article?id=16-Access-Requests-by-Public-Authorities.

US DEP'T OF COMMERCE, PRIVACY SHIELD FRAMEWORK, *How to Submit a Request Relating to U.S. National Security Access to Data* (2016), https://www.privacyshield.gov/article?id=How-to-Submit-a-Request-Relating-to-U-S-National-Security-Access-to-Data.

US DEP'T OF HEALTH AND HUMAN SERVICES, *Cignet Health fined a $4.3M Civil Money Penalty for HIPAA Privacy Rule Violations*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cignet-health/ (last visited Oct. 19, 2016).

US DEP'T OF HEALTH AND HUMAN SERVICES, *Enforcement Highlights*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

US DEP'T OF HEALTH AND HUMAN SERVICES, *Enforcement Results by Year*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html.

US DEP'T OF HEALTH AND HUMAN SERVICES, *HIPAA Privacy, Security, and Breach Notification Audit Program*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/#program (last visited Oct. 19, 2016).

US DEP'T OF HEALTH AND HUMAN SERVICES, *How OCR Enforces the HIPAA Privacy & Security Rules*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html.

US DEP'T OF HEALTH AND HUMAN SERVICES, *Massachusetts General Hospital Settles Potential HIPAA Violations*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/massachusetts-general-hospital/index.html.

US DEP'T OF HEALTH AND HUMAN SERVICES, *Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC)*, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/UMMC/index.html.

US DEP'T OF HEALTH AND HUMAN SERVICES, *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/.

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Amici Curiae*, http://www.fisc.uscourts.gov/amici-curiae.

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Public Filings*, http://www.fisc.uscourts.gov/public-filings.

U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE, HOUSE.GOV, http://intelligence.house.gov/.

U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE, *History and Jurisdiction*, HOUSE.GOV, http://intelligence.house.gov/about/history-and-jurisdiction.htm.

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

Worldwide Cyber Threats: Hearing before the H. Permanent Select Comm. on Intelligence, 114th Cong. 2 (Sept. 10, 2015) (statement of James R. Clapper, Dir. of National Intelligence), https://fas.org/irp/congress/2015_hr/091015clapper.pdf.

State

FLORIDA OFFICE OF THE ATTORNEY GENERAL, *Attorneys General Reach Settlement with Zappos over Data Breach* (Jan. 7, 2015), http://www.myfloridalegal.com/newsrel.nsf/newsreleases/F12E26235A23E57785257DC60063AEE9.

KAMALA D. HARRIS, ATTORNEY GENERAL CALIFORNIA DEPARTMENT OF JUSTICE, CALIFORNIA DATA BREACH REPORT (2016), https://oag.ca.gov/breachreport2016.

NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL, *New York State Security Breach Reporting Form*, https://forms.ag.ny.gov/CIS/breach-reporting.jsp.

NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL, *A.G. Schneiderman Announces Settlement with Trump Hotel Collection after Data Breaches Expose over 70K Credit Card Numbers* (Sept. 23, 2016), http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-trump-hotel-collection-after-data-breaches-expose.

Privacy Enforcement Actions, STATE OF CALIFORNIA OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/privacy/privacy-enforcement-actions.

Security Breach Notification Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

STATE ATTORNEYS GENERAL: POWERS AND RESPONSIBILITIES (Emily Myers, Nat'l Ass'n of Attorneys General eds., 3d ed. 2013).

STATE OF CALIFORNIA OFFICE OF THE ATTORNEY GENERAL, *Consumer Complaint Against a Business/Company*, https://oag.ca.gov/contact/consumer-complaint-against-business-or-company.

VI. OTHER STATES

Statutes and Codes

Закон за специалните разузнавателни средства [Bulgaria Special Intelligence Means Act], Oct. 21, 1997, Нов - ДВ, бр. 109 от 2008 г., изм. - ДВ, бр. 70 от 2013 г., в сила от 09.08.2013 г. [as amended by SG. 109 of 2008, SG. 70 of 2013, effective Aug. 9, 2013] (Bulg.).

Bundesgesetz über den Schutz personenbezogener Daten [Federal law on the Protection of Personal Data] (Datenschutzgesetz 2000 (DGS2000)) [(Data Protection Act 2000 (DGS2000), as amended)] Bundesgesetzblatt [BGBl] No. 165/1999, as amended (Austria).

CODE DE LA DÉFENSE [DEFENSE CODE], Arts. R.*1132 *et seq.* (Fr.), (in French) https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307.

CODE DE LA SÉCURITÉ INTÉRIEURE [INTERIOR SECURITY CODE], Art L. 851-3 (Fr.), *La localisation, la sonorisation de certains lieux et véhicules, la captation d'images et de données informatiques*, http://www.assemblee-nationale.fr/14/projets/pl2669.asp.

CODE DES RELATIONS ENTRE LE PUBLIC ET L'ADMINISTRATION [CODE OF RELATIONS BETWEEN THE PUBLIC AND THE ADMINISTRATION], Art. L. 311-5, (in French) https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000031366350&idArticle=LEGIARTI000031367708.

CODE PÉNAL [PENAL CODE], Art. 413, (in French) https://www.legifrance.gouv.fr/affichCode.do;jsessionid=2704B41AAA557321BFC3F6F7614388CF.tpdila11v_3?idSectionTA=LEGISCTA000006165357&cidTexte=LEGITEXT000006070719&dateTexte=20161031.

Gesetz über den Bundesnachrichtendienst [BNDG] [German Act on the Federal Intelligence Service], Dec. 21, 1990, das zuletzt durch Artikel des Gesetzes vom 26. Juli 2016 (BGBI. I.S.1818) [last amended by Art.2 of the Law of July 26, 2016 (I, at 1818)].

Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG) [German Federal Act on the Protection of the Constitution] Dec. 20, 1990, das zuletzt durch Artikel des Gesetzes vom 26. Juli 2016 [last amended by Article 1 of the Law of July 26, 2016 (I, at 1818)], (in German) https://www.gesetze-im-internet.de/bverfschg/BJNR029700990.html.

Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz - IFG), [Freedom of Information Act] Sept. 5, 2005, das durch Artikel 2 Absatz 6 des Gesetzes vom 7. August 2013 [as amended by Article 2 Paragraph 6 of the Law of Aug. 7, 2013] (BGBl. I S. 3154) (Ger.), (in German) https://www.gesetze-im-internet.de/bundesrecht/ifg/gesamt.pdf.

Justice and Security Act 2013 c. 18 (UK), http://www.legislation.gov.uk/ukpga/2013/18/pdfs/ukpga_20130018_en.pdf.

Legge 124/2007: Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto [Law no. 124/2007 [System of Intelligence for the Security of the Republic and New Provisions on Secrecy] (It.), (in English) https://www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html.

Loi 98-567 du 8 juillet 1998 instituant une Commission consultative du secret de la défense nationale (1) [Law of 8 July 1998 Instituting a Consultative Commission on National Defense Secrets (1)], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [OFFICIAL GAZETTE OF FRANCE] July 9, 1998, p.10488, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000389843&categorieLien=id.

Official Secrets Act 1989, c. 6 (U.K.), http://legislation.data.gov.uk/ukpga/1989/6/data.htm?wrap=true.

Regulation of Investigatory Powers Act 2000, c. 23 (U.K.), http://www.legislation.gov.uk/ukpga/2000/23/contents.

Case Law

Balfour v. Foreign and Commonwealth Office [1993] ICR 663 (E.A.T.) (UK), http://www.bailii.org/uk/cases/UKEAT/1993/182_92_1210.html.

Balfour v. Foreign and Commonwealth Office [1994] 2 All ER 588, [1994] 1 W.L.R. 681 (C.A.) (UK).

BVerfG [Federal Constitutional Court], decision of the First Senate of 27 October 1999, 1 BvR 385/90 (Ger.), (in German) https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1999/10/rs19991027_1bvr038590.html.

BVerwG [Supreme Administrative Court], judgment of 26 August 2004, BVERWG 20 F 19.03 (Ger.), (in German) http://www.bverwg.de/entscheidungen/entscheidung.php?ent=260804B20F19.03.0.

Conseil Constitutionnel [CC] [Constitutional Council], decision No. 2011-192 QPC, Nov. 10, 2011 ("*Ekaterina*"), (in English) http://www.conseil-constitutionnel.fr/conseil-constitutionnel/english/case-law/decision/decision-no-2011-192-qpc-of-10-november-2011.104102.html.

Conway v Rimmer [1968] AC 910 (H.L.) (UK), http://www.bailii.org/uk/cases/UKHL/1968/2.html.

Corte Constituzionale [Constitutional Court], 11 marzo 2009, Judgment 106/2009 ("*Abu Omar*"), (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2009&numero=106.

Corte Constituzionale [Constitutional Court] 29 febbraio 2012, Judgment 40/2012 ("*Abu Omar*"), (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2012&numero=40.

Corte Constituzionale [Constitutional Court] 19 febbraio 2014, Judgment 24/2014 ("*Abu Omar*"), (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2014&numero=24.

Duncan v. Cammel Laird & Co. Ltd. [1942] AC 624 (H.L.) (UK), http://www.bailii.org/uk/cases/UKHL/1942/3.html.

Rechtbank Den Haag [Court of the Hague] 23 juli 2014, ECLI:NL:RBDHA: 2014: 8966 (C/09/455237/HA ZA 13-1325, *Dutch Association Criminal Lawyers / Netherlands*) (Neth.), (in Dutch) http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2014:8966.

Sec. of State for Home Dep't v. Davis [2015] EWCA (Civ) 1185 (C.A.) (UK).

VERWALTUNGSGERICHTSORDNUNG, [VWGO] [CODE OF ADMINISTRATIVE COURT PROCEDURE] [CACP] (Ger.), (in English) https://www.gesetze-im-internet.de/englisch_vwgo/englisch_vwgo.html.

Wet op de inlichtingen - en veiligheidsdiensten 2002 7 februari 2002 [Intelligence and Security Act 2002, Feb. 7, 2002] (Neth.).

Reports

DATAINSPEKTIONEN [DATA INSPECTION BOARD], DATAINSPEKTIONENS REDOVISNING AV REGERINGSUPPDRAGET [DATA INSPECTION REPORT OF THE GOVERNMENT COMMISSION], Fö2009/355/SUND, Dec. 6, 2010, (Swed.).

DAVID ANDERSON, A QUESTION OF TRUST: A REPORT OF THE INVESTIGATORY POWERS REVIEW PRESENTED TO THE PRIME MINISTER PURSUANT TO SECTION 7 OF THE DATA RETENTION AND INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT (June 2015) (UK), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK (Mar. 2015) HC 1075 (UK), *visit* http://isc.independent.gov.uk/committee-reports/special-reports *and click on* "Privacy and Security: a modern and transparent legal framework."

MINISTÈRE DE LA DÉFENSE [DEFENSE MINISTRY], SECRÉTARIAT GÉNÉRAL POUR L'ADMINISTRATION [SECRETARY-GENERAL FOR ADMINISTRATION], *Secret Défense* [Defense Secret] (Sept. 17, 2012), (in French) http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/secret-defense/secret-defense.

VII. NON-GOVERNMENTAL SOURCES

Books and Academic Articles

[1 THE SPIRIT OF LAWS] CHARLES LOUIS DE SECONDAT, BARON DE MONTESQUIEU, *Book XI Ch. VI – Of the Constitution of England*, COMPLETE WORKS (1748), http://oll.libertyfund.org/titles/837.

[2 PRINCIPLES FOR CLASSIFICATION OF INFORMATION] ARVIN S. QUIST, SECURITY CLASSIFICATION OF INFORMATION (1993), https://fas.org/sgp/library/quist2/chap_7.html#1.

Alexandra Cumings & Kaplan v. Conyers, *Preventing the Grocery Store Clerk from Disclosing National Security Secrets*, 119 PENN ST. L. REV. 553 (2014).

Andrew E. Nieland, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1202 (2007), http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=3073&context=clr.

Ann Bartow, *Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China*, 74 OHIO ST. L.J. 853 (2013), http://digitalcommons.pace.edu/lawfaculty/922.

CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007).

COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE (2008).

CRISTINA BLASI CASAGRAN, GLOBAL DATA PROTECTION IN THE FIELD OF LAW ENFORCEMENT: AN EU PERSPECTIVE (2017).

Dana Carver Boehm, *Guantanamo Bay and the Conflict of Ethical Lawyering*, 117 PENN ST. L. REV. 283 (2012).

DANIEL J. SOLOVE & PAUL SWARTZ, INFORMATION PRIVACY LAW (4th ed. 2015).

Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583 (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

Danielle Keats Citron, *Privacy Policymaking of State Attorneys General*, NOTRE DAME L. REV. (forthcoming), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.

Federico Fabrinni, *Human Rights in the Digital Age: The European Court of Justice Ruling in Digital Rights Ireland and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUM. RTS J. 65 (2015), http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf.

Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by requiring government access to all data and communications*, MIT COMP. SCI. AND ARTIF. INTEL. LAB. (July 6, 2015), http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

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

Jason B. Jones, *The Necessity of Federal Intelligence Sharing with Sub-Federal Agencies*, 16 TEX. REV. L. & POL. 175 (2011).

JOHN EARL HAYNES AND HARVEY KLEHR, VENONA: DECODING SOVIET ESPIONAGE IN AMERICA (2000).

KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015).

Laura Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POLICY 117 (2015), http://scholarship.law.georgetown.edu/facpub/1355/.

Laura Donohue, *The Fourth Amendment in a Digital World*, 83 U. CHI. L. REV. (forthcoming 2016), http://ssrn.com/abstract=2726148.

M. Cayford, et al., *All Swept Up: An Initial Classification of NSA Surveillance Technology*, in SAFETY AND RELIABILITY: METHODOLOGY AND APPLICATIONS, 643-650 (Nowakowski, et al. eds. 2015), http://www.crcnetbase.com/doi/pdfplus/10.1201/b17399-90.

Martin Schwartz, *Section 1983 Litigation*, FEDERAL JUDICIAL CENTER (2014), https://www.casd.uscourts.gov/Attorneys/CJAAppointments/SiteAssets/docs/FJCSection1983Outline.pdf.

MICHAEL KLARMAN, FROM JIM CROW TO CIVIL RIGHTS: THE SUPREME COURT AND THE STRUGGLE FOR RACIAL EQUALITY (2004).

Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448 (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033207.

Peter Swire, *Markets, Self-Regulation, and Legal Enforcement in the Protection of Personal Information*, SOC. SCI. RESEARCH NETWORK, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=11472.

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

Peter Swire, *Public Feedback Regulation: Learning to Govern in The Age of Computers, Telecommunications, and the Media* (1993) (unpublished), http://peterswire.net/archive/feedback-93.htm.

Peter Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 260 (2006), http://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1195&context=vlr.

Peter Swire, *The Declining Half-Life of Secrets and the Future of Signals Intelligence*, New America Cybersecurity Fellows Paper Series No. 1, NEW AMERICA (July 2015), https://static.newamerica.org/attachments/4425-the-declining-half-life-of-secrets/Swire_DecliningHalf-LifeOfSecrets.f8ba7c96a6c049108dfa85b5f79024d8.pdf.

Peter 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.

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.

Peter Swire & Justin Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, N.Y.U. ANN. SURVEY AM. L. (forthcoming 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728478.

Peter Swire, Justin Hemmings & Suzanne Vergnolle, *Mutual Legal Assistance Case Study: The United States and France*, WISC. INT'L L.J. (forthcoming 2016).

Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416 (2012).

PETER SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS, AND PRACTICES (2012).

PETER SWIRE & KENESA AHMAD, U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS, INT'L ASSOC. OF PRIV. PROF. (2012) https://iapp.org/media/pdf/certification/cippus-us-private-sector-ch3.pdf.

PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335 (2013), http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3550&context=mlr.

RESTATEMENT (SECOND) OF TORTS, (AM. LAW INST. 1965).

Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 234 (2007), https://ssrn.com/abstract=963998.

SUN TZU, THE ART OF WAR, *Ch. 13, The Use of Spies* (5th Century B.C.E.), http://suntzusaid.com/book/13.

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 (2008), http://lsr.nellco.org/columbia_pllt/08155/ (quoting Keith, 407 U.S. at 316-17).

Walter F. Pratt, *Judicial Disability and the Good Behavior Clause*, 85 YALE L.J. 706 (1976), http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1164&context=law_faculty_scholarship.

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

Reports by Non-Governmental Organizations

AMERICAN CIVIL LIBERTIES UNION, *Section 215 Documents*, https://www.aclu.org/foia-collection/section-215-documents.

Bert-Jaap Koops, *Crypto Law Survey, Overview per country, Version 27.0*, CRYPTOLAW.ORG (Feb. 2013), http://www.cryptolaw.org/cls2.htm.

CENTER FOR DEMOCRACY AND TECHNOLOGY, *National Security Standards by Country* (2013), https://govaccess.cdt.info/standards-ns-country.php.

DENNY ANTONIALLY AND JACQUELINE DE SOUZA ABREU, STATE SURVEILLANCE OF COMMUNICATIONS IN BRAZIL AND THE PROTECTION OF FUNDAMENTAL RIGHTS, ELECTRONIC FRONTIER FOUNDATION (Dec. 2015), https://www.eff.org/files/2015/12/17/brazil-en-dec2015_0.pdf.

ELECTRONIC PRIVACY INFORMATION CENTER, *EPIC Administrative Procedure Act (APA) Comments*, EPIC.ORG, https://epic.org/apa/comments/.

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

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

NECESSARY AND PROPORTIONATE, *July 2013 version: International Principles on the Application of Human Rights to Communications Surveillance* (July 10, 2013), https://necessaryandproportionate.org/text/2013/07/10.

PRIVACY INT'L, PRIVACY INTERESTS: MONITORING CENTRAL ASIA SPECIAL REPORT, (Nov. 2014), https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf.

REFORM GOV'T SURVEILLANCE, *Global Government Surveillance Reform: The Principles* (Dec. 9, 2013), https://www.reformgovernmentsurveillance.com/.

RYAN BUDISH, ET AL., NEW AMERICA, OPEN TECHNOLOGY INSTITUTE, HARV. BERKMAN CENTER FOR INTERNET & SOCIETY, *The Transparency Reporting Toolkit* (Mar. 31, 2016), https://www.newamerica.org/oti/policy-papers/the-transparency-reporting-toolkit/

WORLD WIDE WEB FOUNDATION, INDIA'S SURVEILLANCE STATE: COMMUNICATIONS SURVEILLANCE IN INDIA (undated, but content indicates publication post June 2013 Snowden disclosures), http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf.

Non-Governmental Organization Websites

CENTER FOR DEMOCRACY & TECHNOLOGY, *About CDT*, https://cdt.org/about/.

CENTER FOR DEMOCRACY & TECHNOLOGY, *Resources on Data Retention*, (Sept. 26, 2012), https://cdt.org/insight/resources-on-data-retention.

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

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/.

THE IT LAW COMMUNITY, *Not so Safe Harbour: Advocate General's Opinion in Schrems*, SCL.ORG (Sept. 23, 2015), http://www.scl.org/site.aspx?i=ne44089.

News Articles and Other Online Publications

Andrei Soldatov and Irina Borogan**,** *Russia's Surveillance State*, 3 WORLD POLICY INSTITUTE (Fall 2013), http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST (June 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.

Barton Gellman, *U.S. intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST (June 6, 2013), https://www.engadget.com/2013/06/06/washington-post-nsa-fbi-tapping-directly-into-servers-of-9-lea/.

Bryan Preston, *WaPo Quietly Changes Key Details in NSA Story*, PJ MEDIA (June 11, 2013), https://pjmedia.com/blog/wapo-quietly-changes-key-details-in-nsa-story.

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

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.

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.

Declan McCullagh, *No evidence of NSA's 'direct access' to tech companies*, C|NET (June 7, 2013), http://www.cnet.com/news/no-evidence-of-nsas-direct-access-to-tech-companies/.

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/.

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.

GLOBALVOICES, *As Russia insulates itself from human rights bodies, state surveillance decision loom* (Dec. 17, 2015), https://advox.globalvoices.org/2015/12/18/as-russia-insulates-itself-from-human-rights-bodies-state-surveillance-decision-looms/.

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 (June 7, 2013), http://www.businessinsider.com/washington-post-updates-spying-story-2013-6.

Jameel Jaffer, *There Will Be Surveillance Reform*, JUSTSECURITY.COM (Nov. 20, 2014), https://www.justsecurity.org/17622/surveillance-reform/.

James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N. Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

Jedidiah Bracy, *EU Member States approve Privacy Shield*, IAPP.ORG (July 8, 2016), https://iapp.org/news/a/eu-member-states-approve-privacy-shield/.

Jeffrey Meisner, *Microsoft's U.S. Law Enforcement and National Security Requests for Last Half of 2012*, MICROSOFT TECHNET (June 14, 2013), https://blogs.technet.microsoft.com/microsoft_on_the_issues/2013/06/14/microsofts-u-s-law-enforcement-and-national-security-requests-for-last-half-of-2012/.

Jenna Ebersole, *FCC Sets Out Revised Privacy Rules for Broadband Providers*, LAW360 (Oct. 6, 2016), http://www.law360.com/privacy/articles/849021/fcc-sets-out-revised-privacy-rules-for-broadband-providers?nl_pk=dd8be46e-0e43-4bb0-b581-0cbb340d76a6&utm_source=newsletter&utm_medium=email&utm_campaign=privacy.

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/.

Julie Zeveloff, *Webloyalty To Pay Back $10M In Fees In MDL Deal*, LAW360 (Feb. 24, 2009), http://www.law360.com/articles/88713/webloyalty-to-pay-back-10m-in-fees-in-mdl-deal.

Kai Biermann, *BND-Kontrolleure verstehen nichts von Überwachungstechnik [BND Overseers Understand Nothing about Surveillance Technology]*, DIE ZEIT (Oct. 7, 2013), http://www.zeit.de/digital/datenschutz/2013-10/bnd-internet-ueberwachung-provider.

K.C. Jones, *Bank to Pay $50 Million for Buying Personal Data*, INFORMATIONWEEK (Aug. 29, 2006), http://www.informationweek.com/bank-to-pay-$50-million-for-buying-personal-data/d/d-id/1046571.

Ken Dilanian & Courtney Kube, *Top Officials Want to Split Cyber Command From NSA*, NBC NEWS (Sept. 9, 2016), http://www.nbcnews.com/news/us-news/top-officials-want-split-cyber-command-nsa-n645581.

Lauren Raab *et al.*, *Search the Yahoo FISA Case Documents*, L.A. TIMES, http://documents.latimes.com/yahoo-fisa-case/.

Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY (May 11, 2006, 10:38 PM), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

Lev Grossman, *Inside Apple CEO Tim Cook's Fight with the FBI*, TIME MAG. (Mar. 17, 2016), http://time.com/4262480/tim-cook-apple-fbi-2/.

LOVEINT: When NSA officers use their spying power on love interests, WASH. POST (Aug. 24, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/.

HUNTON & WILLIAMS PRIVACY & INFORMATION SECURITY LAW BLOG, *Massachusetts Attorney General Reaches Settlement with Boston Hospital Over Data Security Allegations* (Nov. 25, 2014), https://www.huntonprivacyblog.com/2014/11/25/massachusetts-attorney-general-reaches-settlement-boston-hospital-data-security-allegations/.

Natasha Lomas, *Encryption under fire in Europe as France and Germany call for decrypt law*, TECHCRUNCH, (Aug. 24, 2016) https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/.

Nicole Gaouette, *Intel chief: Presidential campaigns under cyber attack*, CNN.COM (May 18, 2016), http://www.cnn.com/2016/05/18/politics/presidential-campaigns-cyber-attack/.

Pete Brush, *LensCrafters Settles $20 Million Indemnification Battle*, LAW360 (Mar. 31, 2009), http://www.law360.com/articles/94630/lenscrafters-settles-20m-indemnification-battle.

Peter Swire, *Don't Strike Down the Safe Harbor Based on Inaccurate Views About U.S. Intelligence*, IAPP PRIVACY PERSPECTIVES (Oct. 5 2015), https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law.

Peter Swire, *Questions and Answers on Potential Telco Liability*, THINK PROGRESS (May 12, 2006), https://thinkprogress.org/questions-and-answers-on-potential-telco-liability-e5fa4bdd4c0d#.1qokc850w.

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.

Peter Swire, *Solving the Unsolvable on Safe Harbor – the Role of Independent DPAs*, IAPP PRIVACY PERSPECTIVES (Oct. 13 2015), https://iapp.org/news/a/solving-the-unsolvable-on-safe-harbor-the-role-of-independent-dpas.

Peter Swire, *The USA Freedom Act, the President's Review Group, and the Biggest Intelligence Reform in 40 Years*, IAPP PRIVACY PERSPECTIVES (June 8, 2015), https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years.

Pierluigi Paganini, *New powers for the Russian surveillance system SORM-2*, SECURITY AFFAIRS (Aug. 18, 2014), http://securityaffairs.co/wordpress/27611/digital-id/new-powers-sorm-2.html.

Pranesh Prakash, *How Surveillance Works in India*, N. Y. TIMES (July 10, 2013), http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india.

Richard Lawler, *Washington Post: NSA, FBI tapping directly into servers of 9 leading internet companies (update)*, ENGADGET (June 6, 2013), https://www.engadget.com/2013/06/06/washington-post-nsa-fbi-tapping-directly-into-servers-of-9-lea/.

Suevon Lee, *Sprouts' W2 Leak In Data-Phishing Scam Prompts Suit*, LAW360 (Apr. 21, 2016), http://www.law360.com/articles/787592.

Tim Cushing, *FISA Court's Appointed Advocated Not Allowing Government's 'National Security' Assertions To Go Unchallenged*, TECHDIRT.COM (Dec. 11, 2015), https://www.techdirt.com/articles/20151210/08175733048/fisa-courts-appointed-advocate-not-allowing-governments-national-security-assertions-to-go-unchallenged.shtml.

The Watergate Story, WASH. POST SPECIAL REPORTS, http://www.washingtonpost.com/wp-srv/politics/special/watergate/.

Tirath Bansal, *Investigatory Powers Bill: Rushed through under Cover of Brexit*, COMPUTERWEEKLY.COM (July 13, 2016), http://www.computerweekly.com/news/450300206/Investigatory-Powers-Bill-rushed-through-under-cover-of-Brexit.

W. Olson, *Regulation through Litigation*, POINTOFLAW (Aug. 30, 2005) http://www.pointoflaw.com/regulation/overview.php.

Business Documents

APPLE, *Transparency Report*, http://images.apple.com/legal/privacy/transparency/requests-2015-H2-en.pdf.

AT&T, *Transparency Report*, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html.

FACEBOOK, *United States Law Enforcement Requests for Data*, GOVERNMENT REQUESTS REPORT (2016), https://govtrequests.facebook.com/country/United%20States/2015-H1.

GOOGLE, *Privacy Policy*, https://www.google.com/policies/privacy/ (last updated Aug. 29, 2016).

GOOGLE, *Transparency Report – United States* (2016) https://www.google.com/transparencyreport/userdatarequests/US/.

MICROSOFT, *Privacy Statement*, https://privacy.microsoft.com/en-US/privacystatement (last updated Sept. 2016).

TWITTER, *Privacy Policy*, https://twitter.com/privacy?lang=en (last updated Sept. 30, 2016).

VODAFONE, LAW ENFORCEMENT DISCLOSURE REPORT: LEGAL ANNEX (June 2014), http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf.

Transparency Report, YAHOO!, https://transparency.yahoo.com/government-data-requests/country/United%20States**/31/?tid=31.

Sound Recordings and Videos

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 July 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.

Privacy in the EU and US: A Debate between Max Schrems and Peter Swire, SOUNDCLOUD, https://soundcloud.com/justin-hemmings-44462987/privacy-in-the-eu-and-us-a-debate-between-max-schrems-and-peter-swire.

APPENDIX B:

INDEX OF ACRONYMS USED IN TESTIMONY OF PROFESSOR PETER SWIRE

ACLU	American Civil Liberties Union
ADR	Alternative dispute resolution
AG	Attorney General
BCR	Binding Corporate Rule
BND	German Bundesnachrichtendienst
BRIC	Brazil, Russia, India, and China
BSI	Basic Subscriber Information
CACP	German Code of Administrative Court Procedure (Verwaltungsgerichtsordnung)
CalCIPA	California Invasion of Privacy Act
CalECPA	California Electronic Communications Privacy Act
CalOPPA	California Online Privacy Protection Act
CBP	Customs and Border Protection
CCNDS	French Consultative Commission on National Defense Secrets
CEPS	Center for European Policy Studies
CFPB	US Consumer Financial Protection Bureau
CIA	US Central Intelligence Agency
CIPA	Classified Information Procedures Act
CJA	Irish Criminal Justice (Surveillance) Act
CJEU	Court of Justice of the European Union
CLRA	California Consumers Legal Remedies Act
CMIA	California Confidentiality of Medical Information Act
CMP	UK Closed Material Proceeding
CNCIS	French Commission nationale de contrôle des interceptions de sécurité
COPPA	Children's Online Privacy Protection Act

CPNI	Customer proprietary network information
CSO	Court Security Officer
DNI	US Director of National Intelligence
DOD	US Department of Defense
DOJ	US Department of Justice
DOJ NSD	US Department of Justice, National Security Division
DPA	EU Data Protection Authority
ePHI	Electronic Protected Health Information
ECHR	European Court of Human Rights
ECPA	Electronic Communications Privacy Act
ECS	US Department of Homeland Security's Enhanced Cybersecurity Services
EDPS	European Data Protection Supervisor
EFTA	Electronic Funds Transfer Act
EPIC	Electronic Privacy Information Center
EU	European Union
FBI	US Federal Bureau of Investigation
FCC	US Federal Communications Commission
FCRA	Fair Credit Reporting Act
FISA	Foreign Intelligence Surveillance Act
FISC	US Foreign Intelligence Surveillance Court
FISCR	US Foreign Intelligence Surveillance Court of Review
FTC	US Federal Trade Commission
FTCA	Federal Tort Claims Act
GATS	General Agreement on Trade in Services
GCHQ	UK Government Communications Headquarters
HHS	US Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health

IAPP	International Association of Privacy Professionals
IC	US Intelligence Community
IG	Inspector General
ISP	Internet Service Provider
LIBE	European Parliament Committee on Civil Liberties, Justice and Home Affairs
MCT	Multiple Communication Transactions
MFIAC	Yale Law School Media Freedom & Information Access Clinic
MFN	Most Favored Nation
NATO	North Atlantic Treaty Organization
NSA	US National Security Agency
NSD	National Security Division
NSL	National Security Letters
OCR	US Department of Health and Human Services Office for Civil Rights
ODNI	US Office of the Director of National Intelligence
OHSU	Oregon Health & Science University
OIG	US Office of the Inspector General
PAA	Protect America Act
PCLOB	Privacy and Civil Liberties Oversight Board
PHI	Protected Health Information
PII	UK Doctrine of Public Interest Immunity
PPD	Presidential Policy Directive
PR/TT	Pen Register / Trap-and-Trace devices
SAC	German Supreme Administrative Court
SCA	Stored Communications Act
SCC	Standard Contractual Clause
SEC	US Securities and Exchange Commission
SIGINT	Signals Intelligence
SIUN	Sweden, Inspection for Defense Intelligence Operations

TS/SCI	Top Secret / Sensitive Compartmented Information
UCL	California Unfair Competition Law
UDAP	Unfair and deceptive acts and practices
UMMC	University of Mississippi Medical Center
UNDOM	Swedish Intelligence Court
URL	Universal Resource Locator
US	United States of America
USA FREEDOM	Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
VA	US Department of Veterans Affairs