CHAPTER 1:

SUMMARY OF TESTIMONY

Introduction 1-1

Part 1: Biographical Summary for Peter Swire 1-4

Part 2: Systemic Safeguards in US Law and Practice 1-5
I. Systemic Safeguards in Foreign Intelligence 1-6
A. The US as a Constitutional Democracy under the Rule of Law 1-6
B. Statutory Safeguards over Foreign Intelligence Surveillance 1-7
1. The Foreign Intelligence Surveillance Court 1-8
2. Collection of Metadata under Section 215 1-9
3. Collection of Communications under Section 702 1-10
C. Oversight of Surveillance Activities 1-11
D. Transparency Safeguards 1-12
E. Executive Safeguards 1-14
II. Systemic Safeguards in Law Enforcement 1-15
III. Conclusion on Systemic Safeguards 1-16

Part 3: Individual Remedies in US Privacy Law 1-17
I. Individual Remedies Against the United States Government 1-18
A. US Civil Judicial Remedies 1-18
B. US Criminal Judicial Remedies 1-22
II. Non-Judicial Individual Remedies in the US against the US Government 1-23
III. Additional US Privacy Remedies under Federal Law 1-24
IV. Enforcement under US State Law and Private Rights of Action 1-25
V. US Privacy Remedies Concerns in the Irish Data Protection Commissioner's Affidavit 1-25
VI. Conclusions on Individual Remedies, with a Caveat 1-27

Part 4: The Potential Breadth of the Decision and Assessing the Adequacy of Protections for Transfers to the US 1-29
I. The Broad US Definition of "Service Providers" Affected by a Ruling 1-29
II. The US Has Stronger Systemic Safeguards than the BRIC Countries 1-30
III. An Inadequacy Finding for SCCs May Have Implications for Other Lawful Bases for Data Transfers 1-33
IV. Economic Well-Being of the Country 1-35
A. European Union statements about the Importance of the Transatlantic Economic Relationship. 1-35
B. Trade Agreements Including the General Agreement on Trade in Services 1-36
V. National Security 1-37

Part 5: Concluding Discussion 1-39

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.