CHAPTER 2:

BIOGRAPHICAL CHAPTER OF PETER SWIRE

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

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

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

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

---

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

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

[3] Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004), http://peterswire.net/wp-content/uploads/Swire-the-System-of-Foreign-Intelligence-Surveillance-Law.pdf [hereinafter Swire 2004 Paper]. The citation count is based on a search on the term "foreign intelligence" in the Social Science Research Network, www.ssrn.com.

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

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

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

I. Expertise in EU Data Protection Law

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

II. Expertise in US Surveillance Law

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

Annex to Chapter 2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

[23] *Id.* at 78.
[24] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act of 2015), Pub. L. No. 114-23, § 103 (2015), https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf (amending 50 U.S.C. § 1861(b)(2), 1861(c)).
[25] Swire 2004 Paper, *supra* note 3, at 93-94.
[26] USA FREEDOM Act § 401.
[27] *Id.*; 50 U.S.C. § 1803 (i)(2).
[28] USA FREEDOM Act § 401; 50 U.S.C. § 1803 (i)(3).

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

III. The Addition of Adversary Counsel in FISCR Appeals

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

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

IV. Greater Use of Inspector General Oversight after the Fact

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

[49] *Reform*: The Privacy and Civil Liberties Oversight Board (PCLOB) is an independent agency that was established by the Implementing Recommendations of the 9/11 Commission Act in 2007 and fully constituted as an executive agency in 2013.[33] The PCLOB is an independent oversight agency focused on privacy, with the same independent structure as the Federal Trade Commission. In my experience, EU data protection experts have often praised the structure of an independent agency focused on privacy. There are five members, no more than three from any political party, who serve a term of years. Members of the PCLOB and their staff receive Top Secret/Special Compartmentalized Information security clearances and investigate and report on

---

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

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

[31] 50 U.S.C. § 1803.

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

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

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

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

V. Reduced Use of the "Gag Rule"

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

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

---

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

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

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

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

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

[39] Sunset provisions expire unless reauthorized by Congress.

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

VIII. Disclosure of Legal Theories Accepted by the FISC

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

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

IX. Formalization of Minimization Procedures Used by the FISC

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

[63] *Reform:* Presidential Policy Directive 28 (PPD-28), announced in January 2014, addressed minimization procedures. The retention requirements and dissemination limitations in PPD-28, applying to non-US persons, are consistent across agencies and similar to those for US persons.[59] For retention, different intelligence agencies previously had different rules for how long information about non-US persons could be retained. Under the new procedures, agencies generally must delete non-US person information collected through signals intelligence five years after collection.[60] For dissemination, there is an important provision applying to non-US persons: "personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted." [61]

---

[54] THE WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, Presidential Policy Directive, Signals Intelligence Activities, PPD-28 (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28].
[55] USA FREEDOM Act, Pub. L. No. 114-23, § 602 (2015).
[56] Swire 2004 Paper, *supra* note 3, at 97.
[57] 50 U.S.C. §1872(b).
[58] Swire 2004 Paper, *supra* note 3, at 95-96.
[59] The agency procedures create new limits on dissemination of information about non-US persons, and require training in these requirements.
[60] There are exceptions to the five-year limit, but they can apply only after the DNI considers the views of Office of the Director of National Intelligence (ODNI) Civil Liberties Protection Officer and agency privacy and civil liberties officials. *See Signals Intelligence Reform 2015 Anniversary Report*, *supra* note 47.
[61] PPD-28, *supra* note 54, at § 4(a)(i).

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

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

[65] *Reform:* The administration has clearly issued guidelines about limiting surveillance to foreign intelligence purposes. PPD-28 requires paying attention to the privacy of non-US persons and focusing surveillance only on agents of foreign power for legitimate intelligence purposes. PPD-28 states: "Our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information." It adds: "Privacy and civil liberties shall be integral considerations in the planning of US signals intelligence activities." [63]

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

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