Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance

Mieke Eoyang*

Introduction

On a Sunday in September 1975, a young lawyer on the Church Committee named Britt Snider drove to Maryland for a meeting with Dr. Lou Tordella, the retired civilian head of the National Security Agency (NSA). The Committee was investigating an NSA program codenamed SHAMROCK, which collected copies of all telegrams entering and exiting the United States. Tordella told Snider how every day, an NSA courier would hand carry reels of tape from New York to the NSA headquarters at Fort Meade.

According to Tordella, all of the big international telegram carriers cooperated out of a sense of patriotism; they were not paid for their service. Snider suggested that the companies should have known that the government might abuse the situation to spy on American citizens. Tordella warned that the Committee's exposure of the companies' involvement could discourage them and others from cooperating with the government in the future. The companies received assurances from the Attorney General that their conduct was legal. They were nevertheless concerned and sought immunity from prosecution.[1] This episode replayed itself half a century later, when the administration of George W. Bush assured private industry that its involvement in a questionable government surveillance program was perfectly legal.

Surveillance experts often describe the balancing act between the interests of government and the interests of individuals. Frequently left out are the interests of private industry, without which electronic surveillance in the twenty-first century would be impossible. Government intelligence agencies rely on companies who compete in a global market. These firms want to safeguard national security, but must also reassure current and future customers, including those living overseas, that data privacy is a priority. The evolution of statutory surveillance reform has and should continue to reflect these interests.

---

* Mieke Eoyang is the Vice President for the National Security Program at Third Way, and a former professional staff member of the House Permanent Select Committee on Intelligence. The author would like to thank David Forscey for his invaluable research and editing assistance; Ben Wittes for his inspiration to write this article; and the staff of JNSLP for their editorial assistance. This paper would not have been possible without the support and encouragement of the Brookings Institution, the Hoover Institute, and Lawfare.

1. L. Britt Snider, *Unlucky SHAMROCK: Recollections of the Church Committee's Investigation of the NSA*, Studies in Intelligence (Winter 1999-2000), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter99-00/art4.html.

This paper is intended to help frame the issues as Congress considers whether or how to renew the FISA Amendments Act and the particular electronic surveillance programs authorized by that act, colloquially known as "Section 702", which expire on December 31, 2017.[2]

Since the inception of electronic surveillance, and particularly since the 1979 enactment of FISA, private communications providers have acted as the physical and legal gatekeepers separating government and individuals' communications, ensuring that the appropriate process is followed before providing access to the data. Physically, a handover interface is necessary to transfer data from the private sector entity to the requesting government entity in order to provide access for lawful surveillance.[3] Legally, companies are the custodians of their customers' data. They receive the request for the data and hand it over to the appropriate government agency.

This paper will examine national security electronic surveillance through the role of the companies involved—telecommunications companies, Internet service providers, and electronic communications service providers. It focuses on surveillance authorities used to target overseas persons for foreign intelligence purposes. This paper does not cover electronic surveillance in domestic law enforcement or data handling by private entities for commercial purposes.

While the surveillance reform process will consider foreign expectations of privacy and international arrangements for accessing data, the international system for providing information across borders in civil and criminal litigation is distinct from surveillance programs conducted for national security purposes. Thus, this paper does not deal with Mutual Legal Assistance Treaties, or discovery in litigation.

I. LEGAL FRAME

The legal authorities governing U.S. surveillance efforts vary according to the location of the intelligence target and the location of the intelligence collection. The Fourth Amendment and the Foreign Intelligence Surveillance Act (FISA), as amended, work together to regulate collection occurring on U.S. soil against U.S. persons. They guarantee the highest level of privacy protection for potential targets of national security surveillance.

Prior to 2008, collection activities conducted outside the United States against a U.S. person were governed by the Fourth Amendment and Executive Order 12333 (hereinafter EO 12333). EO 12333 acknowledges that intelligence collection activities must respect the rights of U.S. persons,[4] which include U.S.

2. 50 U.S.C. 1801 et seq, P.L. 110-261 (2008), renewed through present in FISA Amendments Act Reauthorization Act of 2012, P.L 112-238 (2012).

3. PAUL HOFFMAN & KORNEL TERPLAN, INTELLIGENCE SUPPORT SYSTEMS: TECHNOLOGIES FOR LAWFUL INTERCEPTS 63 (2005).

4. Exec. Order 12,333 § 1.1(b), 3 C.F.R. 200 (1981), 46 Fed. Reg. 59941 [hereinafter Exec. Order 12,333], *amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003); Exec. Order No.

corporations that are not controlled by a foreign government.[5] It requires the government to "use the least intrusive collection techniques feasible . . . directed against United States persons abroad."[6] However, if overseas collection targets a non-U.S. person, only EO 12333 applies.

As global communications became more interconnected, the legal framework became more complex. In 2008, Congress passed the FISA Amendments Act (FAA) which governs two types of foreign intelligence collection that previously lacked a statutory basis but were occurring within U.S. territory. This surveillance targeted two types of foreign communications traffic: (1) international communications that either started or ended in the United States, i.e., *one-end-domestic* communications and (2) communications between two non-U.S. persons who were outside the United States, i.e., *foreign-to-foreign* communications.[7] Using this new authority, the Intelligence Community (IC) established two new intelligence programs that are now frequently referred to as Prism and Upstream, respectively.

Prism collection allows the government to obtain the content of international communications stored by Internet Service Providers (ISPs), such as Google, Facebook, or Skype. Collected communications must be to or from approved surveillance targets.[8] Under Upstream, the IC copies all email and voice data flowing through the Internet "backbone"—large fiber optic networks owned and operated by private companies [known as "Tier 1" companies,] like AT&T or Level 3 Communications.[9]

While the Fourth Amendment's warrant requirement does not apply to searches or seizures conducted abroad, precisely what rights a non-U.S. person can claim when subject to overseas collection is an unsettled question.[10] However, when

---

13,355, 69 Fed. Reg. 53593 (Aug. 27, 2004); *and* Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008).

5. *Id*. at § 3.5(k).

6. *Id*. at § 2.4.

7. Specifically, Section 702 of the FAA authorized "the Attorney General and the Director of National Intelligence to jointly authorize the (1) targeting of persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information." PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 20 (July 2, 2014) https://www.pclob.gov/library/702-report.pdf [hereinafter PCLOB Report]; *see also* 50 U.S.C. § 1881a(a), (b)(3), (g)(2)(A)(vi) (2012) (amended 2015).

8. PCLOB REPORT, *supra* note 7, at 7.

9. Unlike PRISM, Upstream collects communications that are neither sent nor received by a surveillance target, as long as communications between non-targets reference the target. Upstream also acquires "multiple communications transactions" (MCTs), i.e., email chains, as long as one communication in the MCT is to, from, or about the target. *Id.* at 7, 35-39.

10. Available case law seems clear that the IC does not need an individualized, probable cause search warrant to monitor non-U.S. persons or U.S. citizens overseas for purposes of gathering foreign intelligence. In some circumstances a non-U.S. person may have a Fourth Amendment claim but the law is by no means clear. *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990); United States v. Bin Laden, 126 F. Supp. 2d 264, 285-86 (S.D.N.Y. 2000); *see also* Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 311-12 (Feb. 2015); Corey M. Then, *Searches and*

someone outside of U.S. territory is using a service such as Gmail or iMessage, the corporations that manage those services are entitled to some higher standard of protection. The civil liberties protections enshrined in the Constitution, federal statutes (Section 704 of the FAA), and EO 12333 apply equally to individuals and corporations. Every branch of government has acknowledged a legal and/or prudential concern for the rights of U.S. corporations when they operate overseas.

But in a globalized Internet economy, what should the role of U.S. corporations be, and how does one establish a surveillance framework that respects the companies while permitting the government to fulfill its role in securing the peace?

II. TELECOMMUNICATIONS COMPANIES ARE NECESSARY INTERMEDIARIES FOR ELECTRONIC SURVEILLANCE

The popular communications technologies that have defined the modern world were all developed, owned, and disseminated largely by private industry. From the telegraph to the Internet, private sector companies operate and manage the networks that carry the vast majority of analog and digital traffic.[11] While the early Internet was created and managed by a cooperative of academic researchers, government officials, and non-profits, Congress deliberately privatized this system in 1992.[12] Telecommunications carriers, web development firms, and cloud service providers expanded infrastructure at great expense and with great effort. Today, a global network of private companies links 3.2 billion people[13] who send over 12 billion emails every hour.[14] According to the Internet Association, during 2014 Internet-related firms in the United States

---

Seizures of Americans Abroad: Re-Examining the Fourth Amendment's Warrant Clause and the Foreign Intelligence Exception Five Years After United States v. Bin Laden, 55 DUKE L.J. 1059, 1063-64 (Mar. 2006).

11. Patents gave control of early telegraph networks to private companies, soon dominated by Western Union. In 1876, Alexander Bell filed his patent for a telephone and founded American Telephone and Telegraph (AT&T). AT&T ruled the telephone industry for nearly a century, forging the so-called "Bell System" that would reign until the mid-1980s. *See* ROBERT MACDOUGALL, THE PEOPLE'S NETWORK: THE POLITICAL ECONOMY OF THE TELEPHONE IN THE GILDED AGE 237-39 (Univ. of Pennsylvania Press, 2013); Andrew Pollack, *Bell System Breakup Opens Era of Great Expectations and Great Concern*, NEW YORK TIMES (Jan. 1, 1984), http://www.nytimes.com/1984/01/01/us/bell-system-breakup-opens-era-of-great-expectations-and-great-concern.html.

12. *See generally*, Scientific and Advanced Technology Act of 1992, Pub. L. No. 102-476, Section 4, 106 Stat. 2300 (codified at 42 U.S.C. § 1862(g) (2012)); JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: TELECOMMUNICATIONS LAW AND POLICY IN THE INTERNET AGE 176-77 (2d Edition, MIT Press 2013); TIM WU, THE MASTER SWITCH 168-72, 199-203 (2010).

13. *ITU Releases 2015 ICT Figures*, INT'L TELECOMM. UNION (May 26, 2015), http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx.

14. *Data Never Sleeps* (Infographic), DOMO, https://www.domo.com/learn/infographic-data-never-sleeps (last visited May 30, 2017).

generated $966 billion in revenue—or 6 percent of U.S. GDP.[15]

The Internet changed global telecommunications, introducing challenges and opportunities for U.S. intelligence agencies. Traditionally, a telephone conversation between two people relied on a single, predefined circuit made of copper wires connecting the two parties. This made it easy to eavesdrop on one single call and geographically locate both speakers. Long-distance calling required the signal to cross through "switches" that connected multiple local networks. Because international calling used special international switches, distinguishing domestic calls from international ones was simple.

By contrast, the Internet is a *distributed network*, which resembles a spider web: any two points are connected by *thousands* of potential pathways. If a message cannot take the simplest, shortest path between sender and recipient, it can re-route itself along any other available track. The trip may be longer in terms of distance, but electronic signals travel so fast that the time difference is negligible. Thus, an email might travel around the world to reach a computer less than a mile away.[16]

For the U.S. intelligence community, the emergence of the global Internet was a double-edged sword. On the one hand, it became difficult to distinguish between domestic and international communications; parts of an email exchange between two people living in Atlanta could travel through Cairo. On the other hand, the distributed design of the Internet provided easy access to foreign intelligence once huge volumes of purely international communications began flowing through the United States.

Moreover, a diverse array of telecommunications carriers, Internet Service Providers (ISPs), hardware manufacturers, and software developers work together to make the Internet run. To be able to send an email to your mother, the message passes through the many layers of this communications network. The email is composed on an application layer involving a web browser, an email service provider, and a file transfer protocol. The message is then processed for transmission—digitized, compressed, encrypted. Ready for delivery, it is not sent in a neat envelope with the address on the outside. Rather, it is broken up into fragments, called packets, where envelope information, known as metadata, and the letter itself, known as content, may be all jumbled together. Those packets are then transmitted across a network full of routers and switches, handed off between different network providers—the largest of which are Tier 1 providers. The digitized packets ride on a physical layer of wires, fiber optic cables, modems—actual devices you can see and touch. Thus, a message sent between any two people on the globe may have a part routed through a server in Virginia while another may route through one company's server in Seattle,

15. Stephen Siwek & Economists Incorporated, *Measuring the U.S. Internet Sector* 5 (2015), http://internetassociation./wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf.

16. A globalized Internet could not operate using point-to-point circuit switching alone—it would be impractical to build the number of connections necessary.

while yet another goes through another company's server in Stockholm, depending on the traffic on the network. All this until the packets arrive reassembled on your mother's device, whether it's a desktop computer, laptop, tablet, mobile phone, or watch.

Each link in this communications chain presents an opportunity for intelligence collection. But as Congress and the IC have both recognized, capitalizing on such opportunities requires coordination and a certain degree of trust between the government and private industry.

Unfortunately, trust between industry and the government is at an ebb as a result of a perceived lack of restraint among intelligence agencies in accessing electronic communications. Policymakers should consider the importance of industry's role in electronic surveillance for three reasons. First, intelligence agencies' access to necessary national security information is best done through a voluntary or legally compelled process. The company, not the government, then sorts through the information and provides what is asked for. An adversarial relationship between government and industry means that industry begins putting obstacles in the way of government's access to the information, legal, technological, or otherwise.

Second, when the government does not properly balance the economic concerns with the national security concerns it can harm U.S. competitiveness abroad. For example, the United States had at one point put a limit on the export of high-speed processors to prevent them from falling into the hands of our adversaries. But as computing speeds improved, even home video game systems had processors that exceeded the export control limits, forcing Congress to change the law lest the United States lose that competition to the Japanese market, which had no such restrictions. Forcing U.S. industry to take on security measures not required of its foreign competitors can result in a loss of U.S. competitiveness in the global market.

Finally, as securing consumer's information becomes increasingly important, many companies have internalized the value of privacy as both a competitive matter and as a principle. The rise of hackers, in the form of both criminals and adversary nations, means that customers run the risk of having their identities stolen, their bank accounts raided, their political speech monitored, or their access to information blocked. Increasingly customers have turned to companies, not government, to ensure that their information is safe. Companies have responded by stressing security and privacy as a competitive matter without necessarily differentiating between the motives of those who seek unauthorized access. In that manner, the companies' view of privacy may be closer to that of the user and thus may be a useful proxy for the individual's privacy interest.

III. ROLE OF INTERMEDIARIES IN NATIONAL SECURITY SURVEILLANCE STATUTES

In order to develop policy recommendations to establish an appropriate gatekeeper role for companies, it is useful to look back at the ways that concerns about industry have shaped the national security surveillance frame-

work. Since the Cold War, surveillance statutes have evolved in response to the revelation of controversial electronic surveillance programs. While the relationship between the government and the companies began as informal and voluntary,[17] Congress turned it into a formal, compelled process. After the furor around surveillance programs discovered in the early 70s, lawmakers took some steps to curtail the discretion of the government, while relying on corporate intermediaries to serve as gatekeepers, a pattern that has repeated itself.

A. 1976: FISA

The Church Committee's investigation into SHAMROCK found that the NSA rarely looked at the hundreds of thousands of messages because they were, "too busy keeping up with the real stuff . . . . The program just wasn't producing very much of value."[18] Despite an absence of specific abuse, however, Congressional investigators were struck by the failure of participating companies to spot the potential for abuse, and in hearings into SHAMROCK and one other NSA program, Senator Church described them as "of questionable propriety and dubious legality."[19]

Later, as Congress drafted legislation to curb what it perceived to be abuses by the NSA, the legislation's structure hinged on the role of private companies. Massachusetts Senator Ted Kennedy drafted the Foreign Intelligence Surveillance Act (FISA), which established incentives for private industry to ensure the government followed proper procedures for conducting surveillance with their aid. If the government requested technical assistance from companies without the necessary court order, companies who complied would face civil liability of $1,000 or $100 for every day of violation, as well as punitive damages.[20] Thus, for the first time, Congress placed the companies as gatekeepers between an overzealous government and the privacy rights of individuals.

B. 2001: USA Patriot Act

As lawmakers reacted to the national crisis caused by the attacks on September 11, 2001, they moved to increase the authorities and discretion of the government by passing a very broad Authorization for Use of Military Force as well as a number of additional surveillance authorities in the USA PATRIOT Act.

Section 215 of the PATRIOT Act amended Title V of FISA to authorize federal investigators to compel the production of "any tangible things."[21]

---

17. *See, e.g.*, CHARLIE SAVAGE, POWER WARS 175-76 (2015).

18. Snider, *supra* note 1.

19. *The National Security Agency and Fourth Amendment Rights Before the S. Comm. Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 1-2 (1975) (Opening Statement of Frank Church, Chairman).

20. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, Section 110, 92 Stat. 1796 (codified at 50 U.S.C. § 1810 (2012)).

21. 50 U.S.C. § 1861(a)(1) (2012).

Unbeknownst to the public, the government construed the term "relevant" to authorize the bulk collection of untold volumes of telephone records, called metadata, used to map the social relationships of millions of Americans. But this domestic collection program was not the only bulk surveillance program started after 9/11.

C. TSP: PAA & FAA

On December 16, 2005, the *New York Times* revealed the existence of a warrantless wiretapping program used by the National Security Agency (NSA) to root out suspected terrorists on American soil. Under the Terrorist Surveillance Program (TSP), the government had circumvented the Foreign Intelligence Surveillance Court (FISC) and demanded the assistance of telecommunications providers directly, without a warrant, and had done so for years.[22] President Bush confirmed the program's existence on December 17, acknowledging that the government had been collecting international communications outside of the FISA framework.[23]

The following month, the Electronic Frontier Foundation (EFF) filed a class action lawsuit against AT&T, claiming statutory and punitive damages under FISA.[24] Dozens of other lawsuits were filed against other Tier 1 providers, namely Verizon and Sprint.[25] Given the scope of global communications at issue, the industry suddenly faced a combined liability of hundreds of billions for failing to demand FISA warrants before providing access to customer data.[26] Yet government secrecy prevented the companies from answering the substance

---

22. Soon after the first story, the *Times* reported that the NSA had "gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications." Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES (Dec. 24, 2005), http://www.nytimes.com/2005/12/24/politics/spy-agency-mined-vast-data-trove-officials-report.html.

23. Kelli Arena, *Bush says he signed NSA wiretap order*, CNN, Dec. 17, 2005, http://www.cnn.com/2005/POLITICS/12/17/bush.nsa/.

24. 50 U.S.C. § 1810 allowed individuals that were victim of electronic surveillance or whose information was disclosed or used to seek civil relief. 50 U.S.C. § 1810 (2012). The plaintiffs claimed that AT&T was responsible for seven violations of the law, but only one is relevant to the present discussion. The plaintiffs alleged that AT&T had violated FISA (50 U.S.C. § 1809) either by, "under color of law," engaging in prohibited electronic surveillance and/or intentionally disclosing or using the information obtained. Complaint for Damages, Declaratory, and Injunctive Relief at 30-34, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. C-06-672), 2006 U.S. Dist. Ct. Pleadings LEXIS 2879, *dismissal aff'd sub nom.* NSA Telecomms. Records Litigation v. AT&T Corp., 671 F.3d 881 (9th Cir. 2011).

25. *See* In re National Security Agency Telecommunications Records Litigation, 444 F.Supp.2d 1332 (N.D. Cal. 2006) (describing transfer order).

26. One class of subscribers to Verizon requested $50 billion in damages. John Markoff, *Questions Raised for Phone Giants in Spy Data Furor*, N.Y TIMES (May 13, 2006), http://www.nytimes.com/2006/05/13/washington/13phone.html. *See also* Suchanek v. Sprint Nextel Corp., No. 06-0071 (W.D. Ky. filed May 18, 2006); Dolberg v. AT&T Corp., No. 06-0078 (D. Mont. filed May 15, 2006); Bissitt v. Verizon Commc'ns, Inc., No. 06-0220 (D.R.I. filed May 15, 2006); Herron v. Verizon Global Networks, Inc., No. 06-2491 (E.D. La. filed May 12, 2006); Conner v. AT&T, No. 06-01557 (Cal. Sup. Ct. filed May 12, 2006).

of the legal complaints. As with SHAMROCK, government requests for surveillance assistance had collided with the fear of customer liability.

At first the Bush Administration attempted to gain FISC approval for the program, but even the FISC began to question aspects of the legality of a domestic surveillance program.[27] After several months of going back and forth with the FISC, but ultimately failing to persuade the judges, the Bush administration began negotiations with a newly-Democratic Congress to craft a legislative solution. The result was the Protect America Act of 2007 (PAA), which amended FISA to bring the TSP under statutory authority. The new law supplemented the normal FISA warrant requirement for individualized court orders with a streamlined process that allowed the government to monitor international communications from specific selectors en masse.[28]

PAA would provide a court order that would compel cooperation from companies while shielding them from future liability. As Director of National Intelligence Mike McConnell had told a group of lawmakers prior to passage of the PAA, the IC was willing to accept language providing authority to the FISC, rather than what they had previously received from the Attorney General, to compel provider assistance specifically because it believed that "the companies may not promptly cooperate without a court order given concerns over pending litigation."[29] Going forward, mere certifications from the Executive Branch would not allay company concerns. However, the PAA did not include *retroactive* liability protections for the telecommunications industry; the Bush administration had dropped the idea after initially proposing it in April 2007.[30]

But the issue of retroactive immunity did not die. Bush officials pushed much harder for it during negotiations for a permanent electronic surveillance law—the PAA was a stop-gap measure—and they succeeded.[31] On July 10, 2008, President Bush signed the FISA Amendments Act, which allowed the FISC to compel assistance from electronic communications service providers, while also

27. *See* Cody Poplin, *DOJ Releases Six FISC Documents on Stellar Wind*, LAWFARE (Dec. 15, 2014, 6:44 PM), https://www.lawfareblog.com/doj-releases-six-fisc-documents-stellarwind; *see also* Declassified FISC Ct. Opinion of Judge Roger Vinson (parties redacted), dated April 3, 2007, available at https://www.documentcloud.org//1379006-large-content-fisa-order-documents.html.

28. *See* Protect America Act of 2007, Pub. L. 110-55, §§ 2, 3, 121 Stat. 553 (2007).

29. Letter from Hon. John D. Rockefeller IV, United States Senator, to John Michael McConnell, Director Of National Intelligence, p. 29 (Aug. 29, 2007), https://www.eff.org/files/filenode/foia_C0705278/113007_odni01.pdf.

30. *Cf. Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. (2007) (statement of . . .).

31. Bush made an explicit call for retroactive immunity on October 10. David Jackson & Douglas Stanglin, *Bush Pushes for Telecom Immunity*, USA TODAY (OCT. 10, 2007), https://usatoday30.usatoday.com/news/washington/-10-10-bush-eavesdropping_N.htm. The following February, DNI McConnell went on NPR Radio to tout the importance of retroactive liability as a matter of national security: "The [real] issue is liability protection for the private sector. We cannot do this mission without their help . . . They are being sued for billions of dollars, so the Board's fiduciary responsibilities causes them to be less cooperative . . ." Morning Edition, *Intel Chief: Telecom Immunity a Security Issue*, NPR (Feb. 15, 2008, 6:00 AM), http://www.npr./templates//story.php?storyId=19072207.

providing retroactive liability protections for past violations of FISA.[32]

Retroactive liability emerged as the central obstacle to surveillance reform. Some lawmakers believed that the companies should face the consequences of failing to perform their function as gatekeepers, a role specifically contemplated by FISA. House Democrats in particular expressed concern about the scope of the liability protections.[33] This was the view of California Representative Anna Eshoo, who opposed the bill:

> "Under the original structure of FISA, telecommunications carriers served an important gate-keeping function. They were not permitted to provide access to private communications in the United States unless the government made a lawful request to conduct surveillance, pursuant to a FISA order . . . We all remember the shocking news when [President Bush] had to acknowledge that his Administration created an illegal, warrantless electronic surveillance program outside of the FISA legal framework. This legislation would essentially grant retroactive immunity to telecommunications carriers who relied on statements made by this Administration that the program was lawful . . . There should be at least some minimal inquiry into whether the telecommunications carriers reliance on [administration statements] was reasonable."[34]

Eshoo and others claimed that if the companies received liability protection in this instance, those same firms might expect it in the future, and therefore abdicate their intermediary role.

Ultimately, lawmakers determined that companies should be held harmless for their cooperation with the government, considering they acquiesced in the wake of September 11, 2001 under high pressure to aid counter-terrorism efforts. This was the case even if they did not follow the appropriate FISA process, because retroactive immunity was vital "to encourage electronic communication service providers who acted in good faith . . . to cooperate with the Government when provided with lawful requests in the future."[35]

When the FISA Authorization Act approached its first expiration in 2012, the structure of the bill seemed to have achieved political equilibrium. Even though civil libertarians raised objections to the framework, as they had before, the

---

32. *See* Foreign Intelligence Surveillance Act Amendments of 2008 § 201, 50 U.S.C. § 1885a (2012) (providing retroactive immunity to "electronic communication service provider[s]," including telecom providers, cloud computing services, and backbone operators, who assisted the NSA in accordance with the TSP. This compromise measure provided for court review of assurance given by the administration, and if it found a company received them, it could dismiss the case).

33. Debate in the House revolved around granting retroactive immunity to companies that cooperated with the TSP. Representatives McGovern, Conyers, Lofgren, Barbara Lee, Eshoo, Blumenauer, and Nadler focused almost exclusively on the retroactive immunity provisions. *See* 154 CONG. REC. 103, H5740; H5755; H5760; 5765-66; H5771; H5773 (daily ed. June 30, 2008), https://www.congress.gov/crec/2008/06/20/CREC-2008-06-20.pdf.

34. *Id.* at H5771 (Statement of Rep. Eshoo).

35. S. REP. NO. 110-209, at 10 (2007), http://www.gpo.gov/fdsys/pkg/CRPT-110srpt209/pdf/CRPT-110srpt209.pdf.

intelligence community made the case for the national security value of the program. Classified briefings were given to the appropriately cleared members and staff, and the bill easily passed the House in September (301 to 118) and Senate in December (73 to 23).[36]

But after the reauthorization, a young NSA contractor named Edward Snowden would dramatically change the political landscape and upset the status quo.

D. Snowden: USA Freedom & Section 702

1. Domestic Reaction and Response

In June 2013, Snowden met with three journalists in Hong Kong and handed over a trove of top secret NSA documents. These records became the basis for a series of news stories that described dozens of previously secret U.S. intelligence programs. The first of these stories revealed that U.S. officials were using Section 215 of the PATRIOT Act to collect the metadata on millions of domestic telephone calls from Verizon. The Administration acknowledged the existence of the program but, in the face of immediate outrage from the American public and lawmakers, sought to point out that they were not collecting content.[37]

In March 2014, after adopting executive branch limits on how it handled the information,[38] President Barack Obama expressed a desire to end so-called "bulk collection" under Section 215. He proposed requiring telephone companies to hold customer data for longer periods, instead of delivering it in bulk to government agencies.[39] But it was not until the following year that Congress was able to pass reform legislation: the USA FREEDOM Act.[40] The bill passed

---

36. Vote H569, House of Representatives, H.R. 5949 (2012), https://www.govtrack.us/congress/votes/112-2012/h569; Vote S236, Senate, H.R. 5949 (2012), https://www.govtrack.us/congress/votes/112-2012/s236.

37. Press Release, President Barack Obama, Statement by the President (June 7, 2013), https://www.whitehouse.gov/the-press-office/2013/06/07/statement-president.

38. In January 2014, President Obama implemented two reforms, reducing from three to two the number of "hops" that could be searched and requiring agencies to obtain a finding of reasonable suspicion from a FISC judge before being able to search. *See* Press Release, President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence. Shortly after President Obama announced the modifications, the PCLOB opined that the metadata program as implemented violated Section 215 of the USA PATRIOT Act. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

39. Press Release, President Barack Obama, Statement by the President on the Section 215 Bulk Metadata Program (Mar. 27, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program.

40. The House of Representatives passed the first USA Freedom Act (H.R. 3361) on May 22, 2014, but it went nowhere, despite the urging of a coalition of tech companies. Technology giants including rivals such as Google, Facebook, Apple, and Microsoft quickly joined forces to found the Reform Government Surveillance Coalition. *See* Jon Swartz, *Tech Giants Team up in Anti-Snooping Effort*, USA TODAY (Dec. 10, 2013), https://www.usatoday.com/story/tech/2013/12/09/google-microsoft-

the House with overwhelming bipartisan support on May 13, 2015, followed by the Senate on June 2, 2015.[41]

The USA FREEDOM Act ended bulk collection of domestic metadata by leaving it in the custody of companies, and requiring government investigators to apply for court-ordered access using a "specific selection term to be used as the basis for production."[42] The FISC could not compel companies to disclose metadata without finding a "reasonable, articulable suspicion that a specific selection term is associated with a foreign power [or an agent thereof] engaged in international terrorism."[43]

Technology companies overwhelmingly supported USA FREEDOM. One coalition of trade associations stated that revising Section 215 was vital to "rebuilding the essential element of trust not only in the technology sector but also in the U.S. government."[44] A Symantec spokesman congratulated Congress on striking "the right balance between protecting national security and the privacy of citizens around the world," which would "pave the way to restoring global trust in the ICT industry."[45] Again, Congress had named private companies as gatekeepers, tasked with shielding private customer data from government requests—although this time the government would compensate companies for their efforts.

But the Section 215 metadata program was only the first of the Snowden leaks. The others concerned U.S. electronic surveillance abroad. And the efforts that the U.S. government took to place limits on a domestic collection program did not assuage the concerns of American companies' foreign customers.

2. Overseas Reaction and Response

The USA FREEDOM Act did not address the concerns overseas, which stemmed from press stories describing other intelligence programs targeting non-U.S. persons abroad that had been revealed by Snowden's trove. These included stories alleging that the NSA deliberately undermined encryption standards, secretly implanted eavesdropping equipment in Cisco routers, broke

---

facebook-others-form-reform-government-surveillance-coalition/3914697/. The tech industry soon found a cause in the USA FREEDOM Act, but was unable to lobby successfully for its passage in 2014. *See* Julian Hattem, *Tech's Bad Year in Washington*, THE HILL (Jan. 3, 2015), http://thehill.com/policy/technology/227863-techs-bad-year. On April 30, 2015, the House Judiciary Committee reported the second USA Freedom Act (H.R. 2048). *See* H.R. REP. NO. 114-109, at 10 (2015), https://www.congress.gov/114/crpt/hrpt109/CRPT-114hrpt109-pt1.pdf.

41. Vote H224, House of Representatives, H.R. 2048 (2015), https://www.govtrack.us/congress/votes/114-2015/h224; Vote S201, Senate, H.R. 5949 (2015), https://www.govtrack.us/congress/votes/114-2015/s201.

42. USA FREEDOM Act of 2015, Pub. L. 114-23, § 103(b)(1), 129 Stat. 268 (2015).

43. *Id.* at § 101(a)(3).

44. Letter from the Info. Tech. Indus. Council to John Boehner and Nancy Pelosi (May 11, 2015), http://www.itic.org//f/9/f91f610d-c32b-4f0c-aeff-534544537a7d.pdf.

45. Angela Swartz, *What Silicon Valley Tech Firms Think of the USA FREEDOM Act's Approval*, SILICON VALLEY BUSINESS JOURNAL (June 2, 2015, 10:33PM), http://www.bizjournals.com/sanjose/news/2015/06/02/what-silicon-valley-tech-firms-think-of-the-usa.html.

into the datalinks of Google and Yahoo abroad, and spied on foreign leaders.[46] Unlike the Section 215 program, the U.S. government has not acknowledged the foreign surveillance programs, except those that were authorized by Section 702. Overseas surveillance programs of non-Americans would have fallen under authority granted by EO 12333.

In particular, U.S. companies were upset to learn that the United States was gathering, in secret, data from the networks of electronic communications providers such as Google and Yahoo.[47] The reports of this practice infuriated executives at some of the most important U.S. technology companies.[48] While on the one hand, the companies were compelled by the government to provide data through the front door via FISA orders under Section 702 (PRISM and Upstream), they were being told that the government was stealing additional data through the back, without their authorization. As one technology company employee said, "the backdoor makes a mockery of the front door."[49]

Taken together, the Snowden allegations left the impression that U.S. intelligence professionals were engaged in a wholesale assault on the global Internet. While U.S intelligence officials have repeatedly said that the allegations were not accurate, their ability to debunk them with specificity was limited by the secrecy of the programs themselves. Further, they gave testimony in Congress intending to reassure lawmakers that the alleged programs were focused on foreigners, who did not enjoy the same Constitutional rights as U.S. persons.[50] This merely fanned the flames of controversy abroad, irking U.S. technology companies who were anxious to protect their overseas market share.

While the characterization of the Snowden documents might be inaccurate, there were enough details in them and enough information acknowledged by the government as true that companies began to react to public perceptions that the NSA was out of control. Large technology companies saw two immediate threats. First, the Snowden affair threatened to undermine their dominant position in the overseas hardware market. For some, foreign revenue outpaced

---

46. Snowden's information also suggested that the U.S. government implanted bugs into Cisco routers without the company's permission. *See* Sarah Silbert, *Latest Snowden Leak Reveals the NSA Intercepted and Bugged Cisco Routers*, ENGADGET (May 16, 2014), https://www.engadget.com/2014/05/16/nsa-bugged-cisco-routers/. In addition, some articles alleged that the NSA had deliberately tried to weaken encryption protocols, which would have introduced vulnerabilities around the world. *See*, *e.g.,* Joseph Menn, *Exclusive: Secret Contract Tied NSA and Security Industry Pioneer*, REUTERS (Dec. 20, 2013), http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131221.

47. *See* Dominic Rushe, Spencer Ackerman & James Ball, *Reports That NSA Taps into Google and Yahoo Data Hubs Infuriate Tech Giants*, THE GUARDIAN (Oct. 31, 2013), https://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links.

48. *See id*.

49. Mieke Eoyang, *A Modest Proposal: FAA Exclusivity for Collection Involving U.S. Technology Companies*, LAWFARE: NATIONAL SECURITY LETTERS (Nov. 24, 2014, 8:00AM), https://www.lawfareblog.com/modest-proposal-faa-exclusivity-collection-involving-us-technology-companies.

50. *See* James R. Clapper, Dir. of Nat'l Intelligence, Statement on Activities Authorized Under Section 702 of FISA (June 6, 2013, 10:03PM), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/869-dni-statement-on-activities-authorized-under-section-702-of-fisa.

domestic revenue. In 2015, the largest U.S. technology firms drew 59 percent of their revenue from foreign sales.[51] Second, those companies whose revenues depended on data transactions with overseas customers, such as Google and Facebook, faced legal challenges from foreign governments concerned about the lack of privacy for foreigners.[52]

In addition to legal troubles, U.S. technology companies began to fear economic losses. In a 2013 report on the fallout from the NSA leaks, an American technology trade association estimated the U.S. cloud computing industry could lose as much as $35 billion in lost foreign contracts.[53] In December 2013, a review group convened by President Obama acknowledged that increasing mistrust of the U.S. technology sector could "have adverse effects on overall U.S. economic growth."[54] Indeed, some European companies sought to take advantage of the controversy. Swisscom developed a cloud service specifically designed to keep data safe from foreign governments.[55]

Some will argue that U.S. technology is so dominant that there is no risk of true economic loss and that estimates are speculative. But beyond whether or not the U.S. companies see quantifiable losses, consumer expectations of privacy have heightened post-Snowden, and companies will adapt to those expectations or lose out to those who meet them. More importantly, as foreign governments and regulatory agencies respond to Snowden's allegations, they are creating great uncertainty about the future of trans-Atlantic data flows, and global Internet commerce.

And finally, American companies have spent millions to secure their infrastructure against their own government, moving to encrypt their own internal data, as well as that of their customers. Rivals such as Google, Apple, and Microsoft all joined forces to push for surveillance reform, saying, "It's time for a change."[56]

---

51. More specifically, the report stated that Apple earned 60% of its revenue from overseas and Intel earned 80%. Matt Krantz, 10 U.S. companies take the most foreign money, USA Today Money, July 15, 2015. Available at http://americasmarkets.usatoday.com/2015/07/15/10-u-s-companies-take-the-most-foreign-money/.

52. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650 (judgment Oct. 6, 2015).

53. Daniel Castro, *How Much Will PRISM Cost the U.S. Cloud Computing Industry?*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION 3 (Aug. 2013), http://www2.itif.org/2013-cloud-computing-costs.pdf.

54. LIBERTY AND SECURITY IN A CHANGING WORLD, REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, 212 (Dec. 12, 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

55. Gerry Smith, *'Snowden Effect' Threatens U.S. Tech Industry's Global Ambitions*, THE WORLD POST (Jan. 24, 2014), http://www.huffingtonpost.com/2014/01/24/edward-snowden-tech-industry_n_4596162.html; Caroline Copley, *Swisscom Builds 'Swiss Cloud' as Spying Storm Rages*, REUTERS (Nov. 3, 2013, 10:18AM), http://www.reuters.com/article/us-swisscom-cloud-idUSBRE9A209S20131103.

56. Reform Government Surveillance, *An open letter to Washington* (signed by AOL, Apple Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo) (December 2013), https://www.reformgovernmentsurveillance.com/; *see also* Samuel Gibbs, *Facebook, Google and Apple Lobby for Curb to NSA Surveillance*, THE GUARDIAN (Nov. 17, 2014, 8:28 AM), http://www.theguardian.com/technology/2014/nov/17/facebook-google-apple-lobby-senate-nsa-surveillance (describing the Reform Government Surveillance coalition's efforts to support surveillance reform).

Apple made changes to its operating system to prevent not only government access, but also its own access to a user's device. And at the application layer, a proliferation of smaller companies began producing messaging systems that allowed only the communicants, not the companies themselves, to see the information. Most fundamentally, the attitude of U.S. companies towards cooperating with the government became adversarial. And despite efforts of the U.S. government to improve relations with the companies, especially in Silicon Valley, the relationship with many companies remains strained and litigious.

3. Fallout Moves Beyond the Public: Schrems

Beyond the frustration of the U.S. companies, Europeans began expressing their concerns with U.S. government surveillance through other leverage points, most notably, by calling into question the U.S.-EU Safe Harbor Agreement.

The smooth functioning of a global Internet requires international agreement to allow the data to flow across borders, while still adhering to the standards of each sovereign country. In Europe, that standard is set by Directive 95/46/EC, which prohibits the transfer of personal data to non-EU countries that do not ensure "an adequate level of protection" for that data.[57] The United States and EU had an agreement, the "Safe Harbor" framework, a legal blanket under which technology companies in the United States could import data from EU member states without fear of litigation.[58] Although companies used other mechanisms, such as contracts, to share data "across" the Atlantic, the Safe Harbor proved the most popular—as of October 2015 over 4,000 companies had used it.[59]

In a 2012 report, the European Parliament had worried that the FAA authorized "the [mass] surveillance of [c]loud data of non-U.S. residents," and recommended "further [i]nquiries" into the law's effects.[60] But the report had very little impact, perhaps owing to its passing reference to the FAA, but also probably because the evidence of actual surveillance was lacking. For EU privacy officials, Snowden's revelations supplied the smoking gun validating their concerns.[61]

---

57. Directive 95/46, 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, art. 25, 1995 O.J. (L281) 31, 45-46 (EC), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:&=BG.

58. U.S. DEP'T OF COM., U.S.-EU SAFE HARBOR FRAMEWORK: A GUIDE TO SELF-CERTIFICATION (2013), http://www.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf.

59. Ivana Kottasova, *Europe Cracks Down on U.S. Tech with Data Ruling*, CNN (Oct. 6, 2015, 1:10 PM), http://money.cnn.com/2015/10/06/technology/facebook-privacy-european-union/.

60. Directorate-Gen. for Internal Pol'y, European Parliament, *Fighting Cyber Crime and Protecting Privacy in the Cloud* 48 (2012), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)_EN.pdf.

61. For a fuller account of reactions in the European Parliament, *see* David Wright & Reinhard Kreissl, *European Responses to the Snowden Revelations: A Discussion Paper*, Increasing Resilience in

After the Snowden leaks drew back the curtains on the NSA's PRISM program, forcing the government to acknowledge it, Austrian Max Schrems sued the Irish Data Protection Authority (DPA) to halt Facebook's data transfers between Ireland and the United States. Schrems claimed the NSA's warrantless access to Facebook's data belied the Commission's 2000 determination that U.S. data protection standards were "adequate."[62] The case, decided by the European Court of Justice in October 2015, threw the cross-border data flows into question.

The ECJ ruled that national DPAs have authority to evaluate and halt data transfer arrangements, whether or not the European Commission has blessed them. Equally important, the ECJ invalidated the most recent European Safe Harbor decision because it failed to explain how certain U.S. practices, in particular easy government access to private data, were consistent with the relatively more stringent European standards of data privacy.[63] Although the ECJ did not explicitly mention Section 702, it was widely read as a challenge to the privacy protections in the operations of that statute.[64] While U.S. officials scrambled to explain to their European counterparts the statutory protections in Section 702, it remains unclear whether those protections will be adequate to save the Safe Harbor agreement without additional legislative reforms.

IV. KEY QUESTIONS FOR SURVEILLANCE REFORM

As Congress approaches the next renewal of the FISA Amendments Act, it faces an environment significantly different from its last renewal. First, allegations that the NSA accessed the internal networks of U.S. companies in secret (i.e., outside of PRISM)[65] tainted relations between Washington and Silicon Valley firms, who were frustrated that government officials violated their corpo-

---

Surveillance Soc'ys 7-9 (Dec. 2013), http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf.

62. Schrems v. Data Prot. Comm'r, [2014] IEHC 310 (Ir.), 12-14 https://www.dataprotection.ie/docimages/documents/DOC180614.pdf.

63. Court of Justice of the European Union Press Release No. 117/15, The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid (Oct. 6, 2015), http://curia.europa.eu/jcms/upload/docs//pdf/2015-10/cp150117en.pdf.

64. *See, e.g.*, Danny O'Brien, *No Safe Harbor: How NSA Spying Undermined U.S. Tech and Europeans' Privacy,* ELEC. FRONTIER FOUND., (Oct. 5, 2015), https://www.eff.org/deeplinks/2015/10/europes-court-justice-nsa-surveilance ("There's only one way forward to end this battle in a way that keeps the Internet open and preserves everyone's privacy . . . For the United States, that means reforming Section 702 of the Foreign Intelligence Surveillance Amendments Act, and re-formulating Executive Order 12333."); Sarah St. Vincent, *Making Privacy a Reality: The Safe Harbor Judgment and Its Consequences for US Surveillance Reform*, CDT: Blog (Oct. 26, 2015), https://cdt.org/blog/making-privacy-a-reality-the-safe-harbor-judgment-and-its-consequences-for-us-surveillance-reform/ ("In the absence of reforms to Section 702 . . . any new data transfer agreements between the EU and the US are very likely to be invalidated by the Court. In order to avoid this . . . Congress urgently needs to make thorough reforms to Section 702.").

65. Barton Gellman et al., *How We Know the NSA had Access to Internal Google and Yahoo Cloud Data*, WASH. POST (Nov. 4, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/.

rate integrity by treating them as a foreign adversary.[66] Second, the stories about bulk data collection spooked overseas consumers and companies, particularly in Europe and South America, who began cancelling contracts with American companies and turning to other providers.[67]

Third, the Snowden disclosures supplied grist for litigation that produced the *Schrems* decision. This single ECJ opinion transformed consumer discontent with U.S. companies into a potentially distressing legal obstacle to cross-border data flows. If Safe Harbor 2.0 proves inadequate, *Schrems* may also have dealt an economic blow to smaller U.S. companies who are unable to relocate data infrastructure to Europe. While the decision itself suggested that the court had not heard enough about NSA surveillance to be able to judge the adequacy of U.S. protections, it is unclear whether further explanation of the protections and limits of Section 702 as it stands will be enough to satisfy either the European Commission or the European Court.

In approaching surveillance reform from the perspective of private industry, Congress should ask itself: What changes are necessary to address these three issues?

A. FISA Exclusivity

First, the U.S. government must address allegations that it took advantage of U.S. companies without their knowledge either by accessing their data or modifying their products. More than anything else, these stories have enraged American technology executives. One way to placate companies' concerns is to expand the current FAA framework to cover intelligence activities that take place overseas and involve knowingly collecting data from a U.S. corporate source.

---

66. *See e.g.*, Sean Gallagher, *Googlers say "F*** You" to NSA, Company Encrypts Internal Network*, ARS TECHNICA (Nov. 6, 2013, 3:35 PM), http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/; InfoWorld Staff, *Apple, Cisco, Dell Unhappy Over Alleged NSA Back Doors in Their Gear*, INFOWORLD (Dec. 31, 2013), http://www.infoworld.com/article/2609310/hacking/—cisco—dell-unhappy-over-alleged-nsa-back-doors-in-their-gear.html; Daniel Thomas & Richard Waters, *Cisco Boss calls on Obama to Reign in Surveillance*, FIN. TIMES (May 18, 2014), https://next.ft.com/content/a697c292-de80-11e3-9640-00144feabdc0 (pay wall).

67. *See* Alexandra Hudson, *German Government Cancels Verizon Contract in Wake of U.S. Spying Row*, REUTERS (June 26, 2014, 5:30PM), http://www.reuters.com/article/us-germany-security-verizon-id USKBN0F11WJ20140626; Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, NEW YORK TIMES (Mar. 21, 2014), https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html; Smith, *supra* note 55; *see also Government Access to Information Survey Results*, CLOUD SECURITY ALLIANCE, 2 (July 2013), https://downloads.cloudsecurityalliance.org/initiatives/surveys/nsa_prism/CSA-govt-access-survey-July-2013.pdf.

Specifically, Congress could mandate that whenever the government wants overseas data on foreign customers, which is in the possession of or transmitted by a U.S. company, the government must compel production with a FISC order rather than take it without their knowledge. The company would receive notification that the IC wanted its data. EO 12333 could no longer authorize the clandestine collection of data held within the networks of U.S. companies, even if the interception occurred outside of U.S. territory. The FAA would become the *exclusive means* for obtaining data from U.S. companies in order to conduct electronic surveillance of persons reasonably believed to be outside the United States.

This would leave the IC free to continue to target the information of foreign individuals held by foreign entities under EO 12333. It could rely on other collection methods to obtain the same information, such as a physical search of the target's premises, physical surveillance of the target, wireless signal interception, or human intelligence. It could also use Section 704 of the FAA to target individuals based on probable cause.

But EO 12333 and Section 704 both illustrate that the law recognizes the rights of U.S. persons overseas to be free from unreasonable surveillance. As mentioned above, EO 12333 acknowledges that intelligence collection activities must take place to protect the rights of U.S. persons,[68] which include corporations incorporated in the United States.[69] Section 704 generally prohibits the government from intentionally targeting, for intelligence purposes, a U.S. person who is overseas if he "has a reasonable expectation of privacy" and if the officials would normally need a search warrant to conduct identical activities inside the United States.[70] This kind of surveillance can only be authorized by an ex parte FISC order or an emergency authorization by the Attorney General.[71]

From the companies' perspective, FISA exclusivity would give them confidence that the FAA process was the only avenue by which the U.S. government was intentionally accessing their infrastructure. This would not eliminate the possibility that as their information flows through the infrastructure of other companies or countries, the U.S. government, or another government, might access it elsewhere. But it would restore a sense of forthrightness in the relationship between the U.S. government and its own companies.

Further, extending FISA exclusivity to overseas collection from U.S. companies would allow the U.S. government and the companies to turn to their foreign customers and users and point to the legal process in the FAA as the highest standard in protection from government intrusion that any country provides. Under the FAA, an independent judge would review the executive branch's application for a specific target set of selectors that have relevance to foreign

68. Exec. Order 12,333 § 1.1(b).

69. *Id.* at § 3.5(k).

70. 50 U.S.C. § 1881c(a)(2) (2012).

71. 50 U.S.C. § 1881c(c)-(d) (2012). Notably, however, a FISC order issued under Section 704 can authorize spying on U.S. persons even if they are not connected to terrorism or clandestine intelligence activities. *See* 50 U.S.C. § 1801(b) (2012).

intelligence and counterterrorism and approve them before collection can begin. It means that an independent branch of government—the Congress—has oversight of intelligence collection from U.S. companies, and given that Congress and the President are often of opposing parties, the oversight would not be a partisan rubber stamp. If companies and the government were to agree to transparent reporting structures, then international customers and users would have a sense of just how small a proportion of the total traffic the government was requesting.

B. Reassuring Foreign Customers

Addressing the anxieties of foreign customers is much more complicated because a number of different rationales have been advanced for the concerns of customers and users abroad, and those rationales may shift from country to country and actor to actor. For example, some have argued that the outrage in Europe is pretext for frustration at the dominance of the U.S. telecommunications and Internet industry and privacy arguments are being advanced to hide protectionist motives. If that is true, there is no policy change that would satisfy European concerns. However, given the implications of the *Schrems* decision and the potential for invalidation of the U.S.-EU Safe Harbor agreement, dismissing that concern as pretextual is a gamble with tremendous economic consequences. The question then becomes, what policy change, if any, is necessary to satisfy the privacy concerns of foreign customers?

A core issue at the heart of the post-Snowden debate on surveillance is whether the pre-filter collection of data constitutes a privacy violation. Are individual rights implicated when the government copies the data, filters the data, searches the filtered data, or stores the filtered data? This question applies most clearly to Upstream collection under Section 702, because PRISM collection is already selector-based. As described by the PCLOB, Upstream accesses Internet data off a major "backbone" of fiber optic cables.[72] It then runs the data through two electronic filters.[73] The first removes domestic communications (the collection of which is prohibited by Section 702), and the second narrows communications to those that contain an authorized "selector."[74] The remaining data take is held by the NSA for review, analysis, and dissemination to other agencies (subject to certain restrictions).[75] This reflects the sense of Congress, expressed by the FAA, that for collection of information between two foreigners overseas acquired on U.S. soil, the government could access the entire stream from a company, and sort out for itself what it wanted to look at. The filter, under Upstream, is in government control.

Peter Swire, a member of the President's Review Group on Intelligence and Communication Technologies, has argued that Upstream is sufficiently protec-

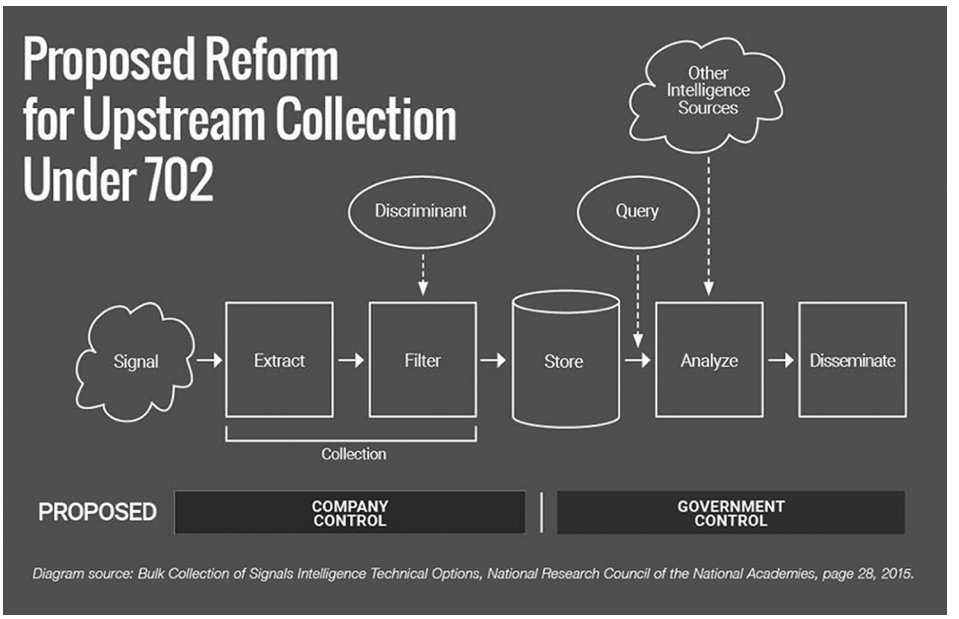
72. PCLOB REPORT, *supra* note 7, at 7.
73. *Id.* at 37.
74. *Id.*
75. *See id.* at 7.

tive of privacy because the data is unexamined until after it has passed through the two filters, and analysts only review a narrow slice of information that is relevant to foreign intelligence.[76]

In other words, analysts can only look at information that is relevant to foreign intelligence.[77]

Given the confusion that exists around the government's access to or possession of the upstream data, Congress should seek to clarify the government's authority, as it has done in amending Section 215. If it is technically possible that the government could only acquire the information after filtering to eliminate the information in which it has no interest, it should do so. Government officials would provide the filters to private companies, who would themselves sift the backbone data and deliver the filtered product to the government.

If the private sector were to take responsibility for the custody and filtering, the government should also compensate the companies for their effort in managing the interface. This would force the government to weigh the relative value of Upstream collection (or potential bulk collection overseas under EO 12333) against the cost of such collection, taking into consideration the cost to the government of filtering such information itself. Changing the custody of the handover interface could resolve numerous privacy concerns while still ensuring that the government could access the relevant information that it needed.



76. *See* Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, FUTURE OF PRIVACY FORUM 2 (Dec. 17, 2015), https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf.

77. *Id.*

While intelligence professionals might challenge modifications to upstream collection, the government has been able to overcome similar objections fairly recently to their efforts to reform a bulk collection program. In the case of the USA FREEDOM Act, the government was able to transition the telephone metadata program operated under Section 215 of the USA PATRIOT Act from one where the government holds the data to one where the companies hold the data, and the government is able to query it for what it needs. If it is technically possible to do in the domestic context, it should be technically possible to do in the foreign context. Moreover, considering the administration's public position, it would be hard-pressed to criticize the transfer of the handover interface into private hands. Surveillance advocates argue that the NSA only accesses the post-filter data—which would be the same data generated by this new procedure.

Rejecting bulk collection in favor of targeted collection, including for overseas communications collected in the U.S., has advantages for the government, the overseas markets, and thus the companies. The Congress should consider making this change for prudential reasons.

From the government's perspective, bulk collection is inefficient. It must establish data centers and storage capacity to hold an entire stream of communications when it is only interested in a small fraction of that stream and the bulk of it is never examined. Further, as an increasing proportion of upstream traffic is encrypted in transit, upstream collection becomes less and less readable. The government must waste processing power to sort through the stream in order to identify the things that it needs. It would more efficient for the government to receive a stream after filtering instead of taking custody of the data before anyone has eliminated the surplus material.

Taking custody only after filtering could also reassure privacy advocates that the government has eliminated one area of potential abuse, that is, that the government, in retaining the bulk data, might use it for a purpose beyond the original authorization—no matter how strong the controls are. Regardless of what the NSA actually does in practice, it has paid a price in suspicion and concern from a public that remembers past misconduct. Given the history of the NSA before FISA, and again in the wake of September 11, 2001, the public's concerns are not purely hypothetical, even if not applicable to the current operations of the intelligence collection activities. This reform would make a critical difference, depriving the government of the capability to search and store all data scooped off the backbone. It will no longer be a question of whether the NSA is adhering to stated guidelines—it simply will not be able to accomplish what critics of bulk collection fear most.

Finally, a process that allows the government to take custody of the data after filtering rather than before, would more closely align with intelligence collection procedures involving U.S. persons inside the United States. In the United States, the government must obtain a court order (which happens to be a warrant) in order to conduct electronic surveillance. To the extent that any bulk collection is allowed, it is limited to metadata that is left in the hands of private

companies that the government can access. Applying a combination of FISA exclusivity and post-filtering upstream collection, the U.S. government would be allowing foreign intelligence collection on individuals with a court order and only conducting acquiring upstream collection after filtering.

C. Establishing a Working Group on Electronic Surveillance Norms

Going forward, this latest debate will not be the last challenge to electronic surveillance norms and the international community needs a way to address these concerns. The Internet Age has also fundamentally changed the business of espionage. Technology today makes it harder for everyone—individuals and governments alike—to hide their actions online. We are in the middle of a golden age of surveillance where governments can compel production of browser histories, drafts of messages, private online diaries, content and metadata around calls, and location of devices. At the same time, if governments try to collect that information on their own, without the cooperation of the legal custodian, traces of those attempts can be discovered by network administrators, researchers, hackers, security consultants or other governments. In addition, the number of individuals necessary to run a technology surveillance program means that the potential for leaking or inadvertent revelation is high. Governments cannot assume that their surveillance activities will be undiscovered forever, and thus must design programs with consideration for their eventual revelation and the consequences of it.

Unfortunately there is little discussion as to the state of global norms around national security espionage, a sensitive subject. In order to begin the discussion, the U.S. should create a forum for discussion of norms with like-minded foreign governments who share an interest in the growth of global technology and who respect their citizens' privacy.

The problem is clearly most acute in Europe, where the Snowden revelations continue to impact U.S. business and U.S. diplomatic relations with our allies. To be able to discuss the national security implications in light of the economic impacts, the United States should start a NATO-OECD working group to discuss international norms around privacy, security, and trans-border data flows. This would allow the United States and Europe (and some non-European allies) to begin to talk about electronic surveillance norms and ensure that both the security and economic interests are represented in the discussion. Such a working group could advise European data protection authorities on the appropriate controls that should exist within a country, and counsel them on technical aspects in the wake of future controversies over electronic surveillance programs.

CONCLUSION

As Congress approaches the next round of electronic surveillance reform, it must take into consideration the concerns of companies, both to ensure future cooperation, and to protect U.S. competitiveness abroad. In order to ensure

future cooperation, the government needs to take steps to change the current adversarial position of technology companies resulting primarily from allegations that the NSA obtained unauthorized access to their data and/or products. Demonstrating a respect for U.S. corporate integrity by acquiring information through a legally-sanctioned process rather than breaking in, could greatly ease corporate opposition. In order to protect U.S. competitiveness abroad, the United States could end bulk, unfiltered foreign collection in favor of a system that keeps the unfiltered stream in the private sectors' hands and allows the government to see and focus on only the information that is necessary to protect national security. And, finally, to begin a conversation around electronic surveillance norms with our closest allies, establishing a forum to discuss both the economic and security considerations would allow for the development of balanced solutions.

These three steps, taken together, would be a tremendous statement of U.S. commitment to the privacy of individuals around the world, and to the free competition of U.S. businesses in the global marketplace.

***