A HOOVER INSTITUTION ESSAY

Beyond Privacy and Security

THE ROLE OF THE TELECOMMUNICATIONS INDUSTRY IN ELECTRONIC SURVEILLANCE

MIEKE EOYANG

Aegis Paper Series No. 1603

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 that 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 reflected—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. This paper would not have been possible without the support and encouragement of the Brookings Institution, the Hoover Institution, and Lawfare.

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.

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 must serve data to the requesting government entity in order to provide access for lawful surveillance.[2] 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 considerations of foreign expectations of privacy and international arrangements for accessing data will affect the consideration of surveillance reform, 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.

Legal Frame

The legal authorities governing US 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 US soil against US persons. They guarantee the highest level of privacy protection for potential targets of national security surveillance.

Collection activities conducted outside the United States against a US person are governed by the Fourth Amendment and Executive Order 12333 (hereinafter EO 12333). EO 12333 acknowledges that intelligence collection activities must respect the rights of US persons,[3] which include US corporations that are not controlled by a foreign government.[4] It requires the government to "use the least intrusive collection techniques feasible . . . directed against United States persons abroad."[5] However, if overseas collection targets a non-US 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) that governs two types

of foreign intelligence collection that previously lacked a statutory basis but were occurring within US 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-US persons who were outside the United States, i.e., *foreign-to-foreign* communications.[6] Using this new authority, the intelligence community (IC) established two new intelligence programs that are now frequently referred to as Prism and Upstream.

Prism collection allows the government to obtain the content of international communications stored by Internet service providers (ISPs), such as Google, Facebook, and Skype. Collected communications must be to or from approved surveillance targets.[7] Under Upstream, the IC accesses all e-mail 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.[8]

While the Fourth Amendment's warrant requirement does not apply to searches or seizures conducted abroad, precisely what rights a non-US person can claim when subject to overseas collection is an unsettled question.[9] However, when someone outside of US 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 US corporations when they operate overseas.

But in a globalized Internet economy, what should the role of US 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?

Telecommunications Companies Are Necessary Intermediaries for Electronic Surveillance

The popular communications technologies that have defined the modern world were developed, owned, and disseminated largely by private industry. From the telegraph to the Internet, for-profit companies built and continue to manage the networks that carry the vast majority of analog and digital traffic.[10] While the early Internet was created and managed by a cooperative of academic researchers, government officials, and nonprofits, Congress deliberately privatized this system in 1992.[11] 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[12] who send more than 12 billion e-mails every hour.[13] According to the Internet Association, during 2014 Internet-related firms in the United States generated $966 billion in revenue—or 6 percent of US GDP.[14]

The Internet changed global telecommunications in ways that introduced challenges and opportunities for US 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 reroute 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 e-mail might travel around the world to reach a computer less than a mile away.[15]

For the US 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 e-mail exchange between two people living in Atlanta 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, ISPs, hardware manufacturers, and software developers work together to make the Internet run. To be able to send an e-mail to your mother, the message passes through the many layers of this communications network. The e-mail is composed on an application layer involving a web browser, an e-mail 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 referred to collectively as 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, 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 a low point as a result of a perceived lack of restraint among intelligence agencies in accessing electronic communications. Policymakers should consider the perspective of industry in electronic surveillance schemes for three reasons. First, intelligence agencies' access to necessary national security information is best done through voluntary or legally compelled process. Doing so allows the company, not the government, to sort through the information necessary and provide 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.

Second, when the government does not properly balance the economic concerns with the national security concerns it can harm US 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 US industry to take on security measures that its foreign competitors do not have to take can result in a loss of US competitiveness in the global market.

Finally, as securing consumers' information becomes increasingly important, many companies have internalized the value of privacy as both a competitive matter and a principle. The rise of hackers, 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 turn to companies, not government, to ensure that their information is safe. Companies then start to value security and privacy as a competitive matter and may not differentiate based on the motives of those who seek access that is not authorized by the end-user. In that, the companies' view of privacy may be closer to the users' and thus may be a useful proxy for the individual's privacy interest.

Role of Intermediaries in National Security Surveillance Statutes

In order to develop policy recommendations to establish an appropriate gatekeeper role for companies, it's useful to look back at the ways that concerns about industry have shaped the national security surveillance framework. 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,[16] Congress turned it into a formal, compelled process. After the furor around

the surveillance program, lawmakers have taken some steps to curtail the discretion of the government while relying on corporate intermediaries to serve as gatekeepers.

1976 // FISA

The Church Committee's investigation into SHAMROCK found that the NSA rarely looked at the hundreds of thousands of messages because it was "too busy keeping up with the real stuff. . . . The program just wasn't producing very much of value."[17] Despite an absence of specific abuse, however, congressional investigators were struck by the failure of participating companies to spot the potential for abuse. In hearings into SHAMROCK and one other NSA program, Senator Church described them as "of questionable propriety and dubious legality."[18]

Later, as Congress drafted legislation to curb what it perceived to be abuses by the NSA, its 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 industry 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.[19] Thus, for the first time, Congress placed the companies as the gatekeeper between an overzealous government and the privacy rights of individuals.

2001 // USA PATRIOT

As lawmakers reacted to the national crisis caused by the attacks on 9/11, 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."[20] 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.

TSP // PAA & FAA

On December 16, 2005, the *New York Times* revealed the existence of a warrantless wiretapping program used by the NSA to root out suspected terrorists on American soil. Under the Terrorist Surveillance Program (TSP), the government had circumvented the FISC and demanded the assistance of telecommunications providers directly, without a

warrant, and had done so for years.[21] President Bush confirmed the program's existence on December 17, acknowledging that the government had been collecting international communications outside of this FISA framework.[22]

The following month, the Electronic Frontier Foundation (EFF) filed a class action lawsuit against AT&T, claiming statutory and punitive damages under FISA.[23] Dozens of other lawsuits were filed against other Tier 1 providers, namely Verizon and Sprint.[24] 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.[25] Yet government secrecy prevented the companies from answering the substance 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.[26] After failing to persuade the FISC 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.[27]

The law 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 it had previously received from the attorney general in order to compel provider assistance specifically because it believed that "the companies may not promptly cooperate without a court order given concerns over pending litigation."[28] Going forward, mere certifications from the executive branch would not allay company concerns. However, 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.[29]

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 stopgap measure—and they succeeded.[30] On July 10, 2008, President Bush signed the FAA, which allowed the FISC to compel assistance from electronic communications service providers, while also providing retroactive liability protections for past violations of FISA.[31]

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.[32] 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 [administration statements] was reasonable.[33]

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 9/11 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."[34]

When the first sunset of the FISA Authorization Act occurred in 2012, political equilibrium around the structure of the bill seemed to have been reached. Even though civil libertarians raised objections to the framework, as they had before, the 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).[35]

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

Snowden // USA FREEDOM // Section 702

1. Domestic Reaction and Response

In June 2013, Snowden met 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 US intelligence programs. The first was that US 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 sought to reassure Americans that it was not content collection, in the face of immediate outrage from the American public and lawmakers.[36]

In March 2014, after adopting executive branch limits on how it handled the information,[37] 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.[38] But it wasn't until the following year that Congress was able to pass reform legislation: the USA FREEDOM Act.[39] The bill passed the House with overwhelming bipartisan support on May 13, 2015, followed by the Senate on June 2, 2015.[40]

USA FREEDOM ended bulk collection of domestic metadata by leaving it in the custody of companies, requiring government investigators to apply for court-ordered access using a "specific selection term to be used as the basis for production."[41] 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] engaged in international terrorism."[42]

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 US government."[43] 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 [information and communications technology] industry."[44] 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 US electronic surveillance abroad. And the efforts that the US 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

USA FREEDOM did not address the concern overseas, which stemmed from press stories describing other intelligence programs targeting non-US persons abroad from Snowden's trove. These included stories alleging that the NSA deliberately undermined encryption standards, secretly implanted eavesdropping equipment in Cisco routers, broke into the datalinks of Google and Yahoo abroad, and spied on foreign leaders.[45] Unlike the Section 215 program, the US government has not acknowledged the foreign surveillance

programs, except those that were authorized by Section 702. Overseas surveillance programs of non-US persons would have fallen under authority granted by EO 12333.

In particular, US companies were upset by stories that the United States was gathering, in secret, data from the networks of electronic communications providers such as Google and Yahoo.[46] The reports infuriated executives at some of the most important US technology companies.[47] 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 back door makes a mockery of the front door."[48]

Taken together, the Snowden allegations left the impression that the US intelligence professionals were engaged in a wholesale assault on the global Internet. While US intelligence officials have repeatedly said that the allegations were not accurate, their ability to debunk the allegations 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 US persons.[49] This merely fanned the flames of controversy abroad, irking US 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 acknowledged by the government as true that the companies began to react to public perceptions that the NSA was out of control. In that, 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 domestic revenue. In 2015, the largest US technology firms drew 59 percent of their revenue from foreign sales.[50] 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.[51]

In addition to legal troubles, US 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 US cloud computing industry could lose as much as $35 billion in lost foreign contracts.[52] In December 2013, a review group convened by President Obama acknowledged that increasing mistrust of the US technology sector could "have adverse effects on overall US economic growth."[53] 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.[54]

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

Finally, American companies 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."[55] 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 only allowed the communicants, not the companies themselves, to see the information. Most fundamentally, the attitude of US companies toward cooperating with the government became adversarial. And despite efforts of the US 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 US companies, Europeans began expressing their concerns with US government surveillance through other leverage points, most notably by calling into question the US-EU Safe Harbor Agreement.

The smooth functioning of a global Internet requires international agreement to allow 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.[56] The US 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.[57] 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, more than four thousand companies had used it.[58]

In a 2012 report, the European Parliament had worried that the FAA authorized "the [mass] surveillance of [c]loud data of non-US residents" and recommended "further inquiries" into the law's effects.[59] 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.[60]

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 US data protection standards were "adequate."[61] The case, decided by the European Court of Justice (ECJ) 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 US practices, in particular easy government access to private data, were consistent with European standards of data privacy.[62] 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.[63] While US officials scrambled to explain to their European counterparts the statutory protections in Section 702, it remains unclear whether those protections would be adequate to save the Safe Harbor agreement without additional legislative reforms.

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[64] that the NSA accessed the internal networks of US companies in secret (i.e., outside of PRISM) tainted relations between Washington and Silicon Valley firms, who were frustrated that government officials violated their corporate integrity by treating them as a foreign adversary.[65] 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.[66]

Third, the Snowden disclosures supplied grist for litigation that produced the *Schrems* decision. This single ECJ opinion transformed consumer discontent with US 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 US companies who are unable to relocate data infrastructure to Europe. While the decision itself suggested that the court had not heard adequately about NSA surveillance in order to be able to judge the adequacy of US 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?

FISA Exclusivity

First, the US government must address allegations that it took advantage of US companies without their knowledge either by accessing their data or by 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 where collection is knowingly from a US corporate source.

Specifically, Congress could mandate that whenever the government wants overseas data on foreign customers which are in the possession of or transmitted by a US company, the government must compel production with a FISC order rather than take it without the company's 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 US companies, even if the interception occurred outside of US territory. The FAA would become the *exclusive means* for obtaining data from US 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 US 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 US persons,[67] which include corporations incorporated in the United States.[68] Section 704 generally prohibits the government from intentionally targeting, for intelligence purposes, a US person who is overseas if he "has a reasonable expectation of privacy" and if the officials would normally need a search warrant if they were conducting identical activities inside the United States.[69] This kind of surveillance can only be authorized by an *ex parte* FISC order or an emergency authorization by the attorney general.[70]

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

Further, extending FISA exclusivity to overseas collection from US companies would allow the US government and the companies to turn to their foreign customers and users and point to the legal process in FAA as the highest standard in protection from government intrusion, one which no other country provides. Under FAA, an independent judge would review the executive branch's application for a specific target set of selectors that have relevance to foreign 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 US companies; given that Congress and the President are often of opposing parties, the oversight will not be a partisan rubber stamp. Transparency reporting structures agreed to between the companies and the government would give international customers and users some sense of how small a proportion of the total traffic was requested.

Reassuring Foreign Customers

Addressing the anxieties of foreign customers is much more complicated because a number of different rationales have been advanced for the anxiety 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 a pretext for frustration at the dominance of the US 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 US-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 Privacy and Civil Liberties Oversight Board, Upstream accesses Internet data off of major "backbone" fiber optic cables. It then runs the data through two electronic filters. 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." The remaining data "take" is held by the NSA for review, analysis, and dissemination to other agencies (subject to certain restrictions). This reflects the sense of Congress, expressed by the FAA, that for collection of information between two foreigners overseas acquired on US 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.

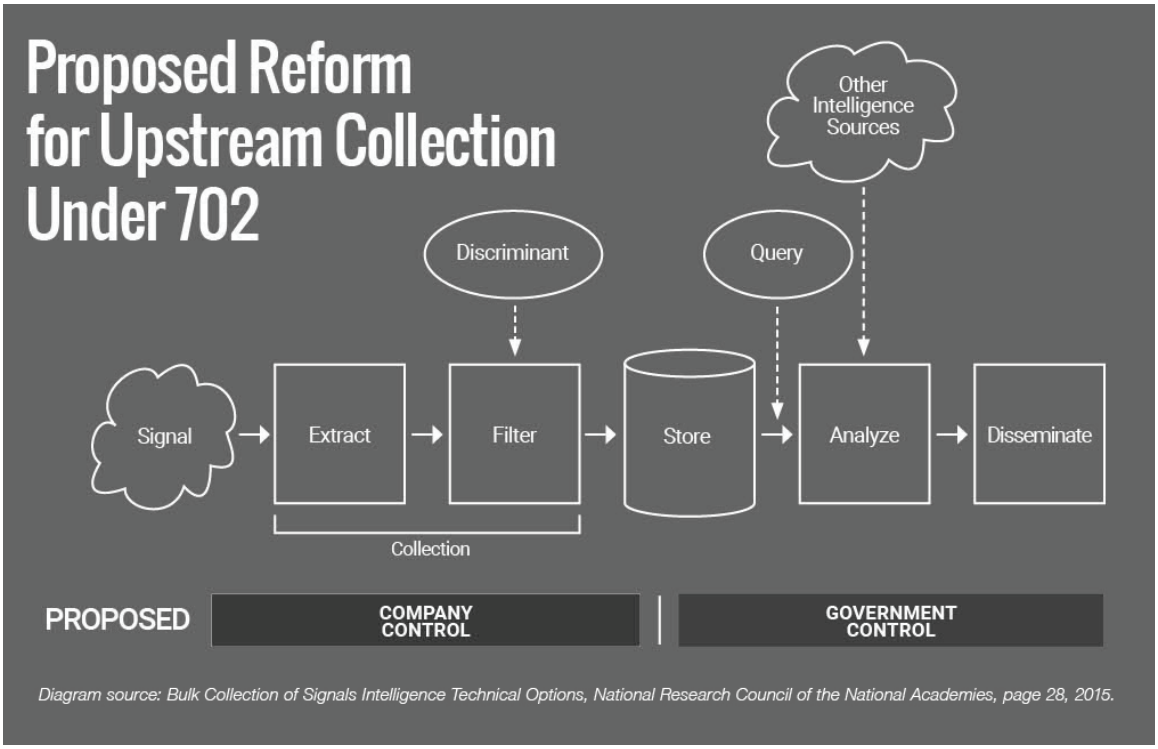

Diagram source: Bulk Collection of Signals Intelligence Technical Options, National Research Council of the National Academies, page 28, 2015.

Peter Swire, a member of the President's Review Group on Intelligence and Communication Technologies, has argued that Upstream is sufficiently protective of privacy because the data is unexamined until after the two filters, and analysts only review a narrow slice of information that is relevant to foreign intelligence.[71] In other words, analysts can only look at information that is relevant to foreign intelligence.[72]

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 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 was able to access the relevant information that it needed.

While intelligence professionals might challenge a modification of Upstream collection, the government has overcome such objections to be able to reform to a bulk collection program, and fairly recently. 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 US, has advantages for the government, the overseas markets, and thus the companies. The Congress should consider doing so 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 in sorting through the stream in order to identify the things that it needs. Receiving a stream after filtering instead of taking custody of the data before anyone in the government would look at it could improve efficiency.

Taking custody only after filtering could also reassure privacy advocates that the government has limited one potential for abuse—eliminating the concern 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 9/11, 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, allowing the government to take custody of the data after filtering, rather than before, would be similar to the framework that applies to US 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 US government would be allowing foreign intelligence collection on individuals with a court order and only conducting acquisition of Upstream collection after filtering.

Establishing a Working Group on Electronic Surveillance Norms

Going forward, this will not be the last challenge to electronic surveillance norms. 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 leaks or inadvertent revelations 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 of the state of global norms around national security espionage, a sensitive subject. In order to begin the discussion, the United States should create a forum for discussion of norms with like-minded foreign governments who share an interest in the growth of global technology and have respect for their citizens' privacy.

The problem is clearly most acute in Europe, where the Snowden revelations continue to impact US business abroad and US 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 working group for members of NATO and the Organisation for Economic Co-operation and Development 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 have both security and economic interests 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 help advise on technical aspects in the wake of future furors over electronic surveillance programs.

Conclusion

As Congress approaches the next round of electronic surveillance reform, it must take into consideration the concerns of the companies, both to ensure future cooperation and to protect US competitiveness abroad. In order to ensure future cooperation, the government must take action that would change the current adversarial position of technology companies that comes mainly from allegations that the NSA obtained unauthorized access to their data and/or products. Demonstrating a respect for US corporate integrity by acquiring information through court processes rather than by breaking in could reduce corporate opposition. In order to protect US competitiveness abroad, the United States could end bulk, unfiltered foreign collection in favor of a system that keeps the unfiltered stream in the private sector's 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 economic and security considerations would allow for the development of balanced solutions.

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

NOTES

1 L. Britt Snider, "Unlucky SHAMROCK: Recollections of the Church Committee's Investigation of the NSA," *Studies in Intelligence,* the Central Intelligence Agency, Winter 1999–2000.

2 Paul Hoffman and Kornel Terplan, *Intelligence Support Systems: Technologies for Lawful Intercepts* (Auerbach Publications, 2006), 63.

3 Executive Order 12333 Section 1.1(b).

4 Executive Order 12333, Section 3.5(k).

5 EO 12333(2.4).

6 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 US 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. 50 U.S.C. § 1881a(a), (b)(3), (g)(2)(A)(vi). See also PCLOB 702 report: 20.

7 Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," 2014 [hereinafter PCLOB Report], http://www.pclob.gov/Library/702-Report-2.pdf.

8 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., e-mail chains, as long as one communication in the MCT is to, from, or about the target. PCLOB Report, 7, 35–41.

9 Available case law seems clear that the IC does not need an individualized, probable cause search warrant to monitor non-US persons or US citizens overseas for purposes of gathering foreign intelligence. In some circumstances a non-US 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); *Bin Laden,* 126 F. Supp. 2d at 285–86; see *generally* Orin Kerr, *The Fourth Amendment and the Global Internet,* 67 Stanford L. Rev. 285 (2015); Corey M. Then, *Searches and 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. 1063–64 (2006).

10 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* (Philadelphia: University of Pennsylvania Press, 2013), 237–39; Andrew Pollack, "Bell System Breakup Opens Era of Great Expectations and Great Concern," *New York Times,* January 1, 1984, http://www.nytimes.com/1984/01/01/us/bell-system-breakup-opens-era-of-great-expectations-and-great-concern.html?pagewanted=all.

11 See generally Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (New York: Knopf, 2010), 168–72, 199–203; Jonathan E. Nuechterlein and Philip J. Weiser, *Digital Crossroads: Telecommunications Law and Policy in the Internet Age,* 2nd ed. (Cambridge, MA: MIT Press, 2013) 176–77; The Scientific and Advanced Technology Act of 1992, Pub. L. No. 102-476, Section 4, 106 Stat. 2300 (codified at 42 USC 1862(g)).

12 http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx.

13 https://www.domo.com/learn/infographic-data-never-sleeps.

14 http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf, pg. 5.

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

16 See, e.g., Charlie Savage, *Power Wars: Inside Obama's Post-9/11 Presidency* (New York: Little, Brown, 2015), 175–176.

17 Snider, *SHAMROCK,* note 1.

18 Opening Statement of Senator Frank Church, Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, October 29, 1975.

19 See FISA of 1978, Pub. L. No. 95-511, Section 110, 92 Stat. 1796 (codified at 50 USC 1810).

20 50 U.S.C. 1861(a)(1).

21 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 and James Risen, "Spy Agency Mined Vast Data Trove, Officials Report," *New York Times,* December 24, 2005.

22 http://www.cnn.com/2005/POLITICS/12/17/bush.nsa.

23 Hepting Complaint, available at: https://www.eff.org/document/eff-complaint-2. 50 USC 1810 allowed individuals who were victims of electronic surveillance or whose information was disclosed or used to seek civil relief. The plaintiffs claimed that AT&T was responsible for seven violations of the law, but only one is relevant to the present discussion. AT&T had violated FISA (50 USC 1809) either by, "under color of

law," engaging in prohibited electronic surveillance and/or intentionally disclosing or using the information obtained. Hepting Complaint at 18-19. Available at: http://www.clearinghouse.net/detail.php?id=12825.

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

25 One class of subscribers to BellSouth and AT&T requested $200 billion in damages. http://www.nytimes.com/2006/05/13/washington/13phone.html?pagewanted=print. For a list of other cases, see 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); 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); Suchanek v. Sprint Nextel Corp., No. 06-0071 (W.D. Ky. filed May 18, 2006).

26 Declassified FISC Opinion of Judge Roger Vinson, dated April 3, 2007, https://www.documentcloud.org/documents/1379006-large-content-fisa-order-documents.html.

27 Protect America Act of 2007, Pub. L. 110-55, §§ 2, 3, 121 Stat. 553.

28 Letter from Senator John D. Rockefeller IV to John Michael McConnell, August 29, 2007, https://www.eff.org/files/filenode/foia_C0705278/113007_odni01.pdf.

29 See http://fas.org/irp/congress/2007_hr/fisamod.html.

30 Bush made an explicit call for retroactive immunity on October 10. "Bush Pushes for Telecom Immunity," *USA Today,* October 10, 2007, http://www.usatoday.com/news/washington/2007-10-10-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," February 15, 2008, http://www.npr.org/player/v2/mediaPlayer.html?action=1&t=1&islist=false&id=19072207&m=19072170.

31 Section 201 of the FAA provided retroactive immunity to "electronic communications service providers," 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. See FAA Section 201 (codified at 50 USC 1885a).

32 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. https://www.congress.gov/crec/2008/06/20/CREC-2008-06-20.pdf at H5740; H5755; H5760; 5765–66; H5771; H5773.

33 Statement of Representative Anna G. Eshoo, June 20, 2008, Congressional Record, H5771 https://www.congress.gov/crec/2008/06/20/CREC-2008-06-20.pdf.

34 http://www.gpo.gov/fdsys/pkg/CRPT-110srpt209/pdf/CRPT-110srpt209.pdf.

35 https://www.govtrack.us/congress/votes/112-2012/s236; https://www.govtrack.us/congress/votes/112-2012/h569.

36 Statement by President Barack Obama, June 7, 2013, the Fairmont Hotel, San Jose, California, https://www.whitehouse.gov/the-press-office/2013/06/07/statement-president.

37 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. President Barack Obama, "Remarks by the President on Review of

Signals Intelligence," January 17, 2014, http://www.whitehouse.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. "Privacy and Civil Liberties Oversight Board, Rep. on the Tel. Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," January 23, 2014 ("PCLOB Report"), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

38 Press Release, The White House, Office of the Press Secretary, "Statement by the President on the Section 215 Bulk Metadata Program," March 27, 2014, http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program.

39 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. Jon Swartz, "Tech giants team up in anti-snooping effort," *USA Today,* December 10, 2013, http://www.usatoday.com/story/tech/2013/12/09/google-microsoft-facebook-others-form-reform-government-surveillance-coalition/3914697/. It soon found a cause in the USA FREEDOM Act, but was unable to lobby successfully for its passage in 2014. 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). H. Rept. 114-109, p. 10, May 8, 2015.

40 http://clerk.house.gov/evs/2015/roll224.xml.

41 H.R. 2048, Section 103(b)(1) (as reported in House 05/08/2015).

42 H.R. 2048, Section 101(a)(3) (as reported in House 05/08/2015).

43 Letter to John Boehner and Nancy Pelosi, May 11, 2015, http://www.itic.org/dotAsset/f/9/f91f610d-c32b-4f0c-aeff-534544537a7d.pdf.

44 Angela Swartz, "What Silicon Valley tech firms think of the USA Freedom Act's approval," *Silicon Valley Business Journal,* June 2, 2015, http://www.bizjournals.com/sanjose/news/2015/06/02/what-silicon-valley-tech-firms-think-of-the-usa.html.

45 Snowden's information also suggested that the US government implanted bugs into Cisco routers, also without the company's permission, http://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, http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131221.

46 http://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links.

47 http://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links.

48 https://www.lawfareblog.com/modest-proposal-faa-exclusivity-collection-involving-us-technology-companies.

49 James R. Clapper, "DNI Statement on Activities Authorized Under Section 702 of FISA," June 6, 2013, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa.

50 More specifically, Apple earned 62 percent of its revenue from overseas and Intel earned 82 percent. Matt Krantz, "10 US companies take the most foreign money," *USA Today Money,* July 15, 2015, http://americasmarkets.usatoday.com/2015/07/15/10-u-s-companies-take-the-most-foreign-money.

51 Maximillian Schrems v. Data Protection Commissioner, Judgment in case C-362/14, October 6, 2015.

52 http://www2.itif.org/2013-cloud-computing-costs.pdf.

53 "The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World," December 12, 2013, 212, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

54 http://www.huffingtonpost.com/2014/01/24/edward-snowden-tech-industry_n_4596162.html; http://www.reuters.com/article/us-swisscom-cloud-idUSBRE9A209S20131103.

55 "Reform Government Surveillance," Open Letter Signed by AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo, Advertisement, *Washington Post,* December 9, 2013, http://www.theguardian.com/technology/2014/nov/17/facebook-google-apple-lobby-senate-nsa-surveillance.

56 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, Article 25(1), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

57 United States Department of Commerce, "U.S.-EU Safe Harbor Framework: A Guide to Self-Certification," March 2013, http://www.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf.

58 http://money.cnn.com/2015/10/06/technology/facebook-privacy-european-union.

59 European Parliament, "2012 Cloud Computing Report," 48, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf.

60 For a fuller account of reactions in the European Parliament, see David Wright and Reinhard Kreissl, "European responses to the Snowden revelations: a discussion paper, Increasing Resilience in Surveillance Societies," December 2013, 7–9, http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf.

61 https://www.dataprotection.ie/docimages/documents/DOC180614.pdf at 12–14.

62 Court of Justice of the European Union, "The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid," Press Release, October 6, 2015., Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

63 See, e.g., Sarah St. Vincent, "Making Privacy a Reality: The Safe Harbor Judgment and Its Consequences for US Surveillance Reform," Center for Democracy and Technology, October 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."); Danny O'Brien, "No Safe Harbor: How NSA Spying Undermined U.S. Tech and Europeans' Privacy," Electronic Frontier Foundation, October 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.").

64 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.

65 http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network; http://www.infoworld.com/article/2609310/hacking/apple--cisco--dell-unhappy-over-alleged-nsa-back-doors-in-their-gear.html.https://next.ft.com/content/a697c292-de80-11e3-9640-00144feabdc0 (may need subscription to access).

66 Claire Caine Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *New York Times,* March 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html; Alexandra Hudson, "German government cancels Verizon contract in wake of U.S. spying row," *Reuters,* June 26, 2014, http://www.reuters.com/article/2014/06/26/us-germany-security-verizon-idUSKBN0F11WJ20140626; Industry survey: https://cloudsecurityalliance.org/research/surveys/#_nsa_prism; http://www.huffingtonpost.com/2014/01/24/edward-snowden-tech-industry_n_4596162.html.

67 Executive Order 12333 Section 1.1(b).

68 Executive Order 12333, Section 3.5(k) (must be revised version, not original 1981 text).

69 50 U.S.C. §1881c(a)(2).

70 50 U.S.C. §1881c(c), (d). Notably, however, a FISC order issued under Section 704 can authorize spying on US persons even if they are not connected to terrorism or clandestine intelligence activities. 50 U.S.C. §1801(b).

71 Swire White Paper presentation to the Belgian Data Protection Authority, December 17, 2015, https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf.

72 Swire White Paper presentation to the Belgian Data Protection Authority, December 17, 2015, https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf.

The preferred citation for this publication is:
Mieke Eoyang, *Beyond Privacy & Security: The Role of the Telecommunications Industry in Electronic Surveillance,* Hoover Working Group on National Security, Technology, and Law, Series Paper No. 1603 (April 8, 2016), available at https://www.lawfareblog.com/beyond-privacy-and-security-role-telecommunications-industry-electronic-surveillance.

About the Author

MIEKE EOYANG

Mieke Eoyang is vice president for the National Security Program at Third Way. She served on the House Permanent Select Committee on Intelligence, conducting oversight leading to the FISA Amendments Act. She was defense policy adviser to Senator Edward M. Kennedy (D-MA) during the Iraq war. She is from Monterey, California, earned her juris doctor at the University of California, Hastings College of the Law, and graduated from Wellesley College.

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200