THIRD WAY

MEMO *Published February 28, 2017 • 20 minute read*

Why Electronic Surveillance Reform is Necessary

Mieke Eoyang
Vice President for the National Security Program
@MiekeEoyang

Gary Ashcroft
2016 Fellow for National Security

Over the next year, Congress will have to address one of the most controversial electronic surveillance statutes, the FISA Amendments Act (commonly referred to by one of its key provisions, Section 702), before it expires at the end of 2017. Legislators will have to wrestle with the public's deep unease with electronic surveillance, given that the U.S. Intelligence Community (IC) consistently argues that Section 702 provides a key tool for national security and will urge its reauthorization. Members of Congress are then faced with the question, "Is reform necessary?"

Section 702 was written to be an important intelligence tool, [1] but drafters did not give sufficient consideration to (1) how the statute is applied in the law enforcement context and (2) how the statute impacts U.S. companies operating in foreign jurisdictions. These two deficiencies have given rise to substantial concerns about the statute at home and abroad, and, in effect, mean that the statutory scheme is "out of balance"; the legitimate security concerns that motivated Section 702 currently outweigh valid concerns related to civil liberties and commerce. During consideration of the statute's reauthorization, Congress has the opportunity to rebalance

these concerns to safeguard Americans' constitutional rights and ensure the continued global competitiveness of U.S. technology companies.

Background

After the terrorist attacks of September 11, 2001, the Bush Administration established a secret electronic surveillance program to collect data and search for terrorist communications. [2] Under that program, known internally as Stellar Wind, Administration officials negotiated with telecommunications companies to obtain, on U.S. soil, their foreign-to-domestic traffic and did so without obtaining court warrants. [3] President Bush acknowledged the existence of the program at the end of 2005, after it was revealed in the media, but Congress did not investigate the program or begin to put statutory controls on it until after the President's party lost control of Congress in the 2006 elections.

Congress passed the Protect America Act (PAA) in 2007 and the FISA Amendments Act, containing Section 702 in 2008. These statutes, which were controversial when they were enacted, aimed to allow the IC to collect needed foreign intelligence and counterterrorism information from U.S. telecommunications and internet companies while also providing additional checks on the IC. In drafting these laws, Congress focused mainly on the legal framework that applies to the IC for its collection abroad.

The IC's legal authority derives from the President's Commander in Chief powers under Article II of the Constitution and is further set out in Executive Order 12333. The focus of the IC's efforts is foreigners abroad, who are not entitled to Constitutional protections. The theory is that if such foreigners are in contact with Americans, the Americans on the other end of the communication cannot assert a privacy interest for those foreigners. Indeed, the warrant requirement usually does not apply to the IC because the intelligence services generally operate against foreigners abroad.

Collection under Section 702 allows elements of the IC to collect data on U.S. soil without a warrant from non-U.S. persons located abroad. Intelligence collection under Section 702 is conducted through two different programs. The first program, known as PRISM, collects communications from what are known as "edge providers," [4] that is, companies that provide Internet content as opposed to Internet connections. The IC obtains access to edge provider communications after the Attorney General and the Director of National Intelligence issue directives, pursuant to guidelines approved by the Foreign Intelligence Surveillance Court, mandating that companies turn over certain information. [5] After these directives are issued, a somewhat obscure branch of the FBI known as the Data Intercept Technology Unit (DITU) coordinates with edge providers, on behalf of the NSA, to collect content such as emails, video chats, and social media posts. This content is then transmitted by the DITU to the NSA, which then disseminates it to other intelligence agencies. [6]

In addition to PRISM, the IC also obtains information through a program called Upstream. Upstream collects "all e-mail and voice data flowing through the Internet 'backbone'—large fiber optic networks owned and operated by private companies like AT&T." [7] The NSA's Special Source Operations (SSO) division partners with the corporate owners of these networks to gather data at certain key points, like at network routers or switches. The companies filter the data passing through these points according to directions they receive from the SSO, and this filtered data is then stored in NSA databases, from which it can be disseminated to other members of the IC. [8]

Although PRISM and Upstream surveillance are similar in many ways, they also exhibit certain key differences. One of the most prominent differences is the type of communications they collect. PRISM only gathers information that is to or from a "selector" – an identifier like an email address, IP address, or social media handle that is associated with a target of foreign intelligence collection.

However, Upstream collects information that is to, from, or about a selector. [9] [10] For example, if the NSA were targeting baddude@qaedamail.com, PRISM collection would only collect communications that were to or from that email address. However, Upstream, in addition to collecting such to or from communications, would also collect any communications that contained the email address baddude@qaedamail.com, even if they weren't to or from that address. Upstream also collects multi-communication transactions (MCTs), which are bundles of communications of which one or more communications may be to, from, or about a targeted selector.

The scope of PRISM and Upstream cannot be overstated. These programs sift through massive quantities of data in an effort to find terrorist communications. in doing so, they are able to look at far more information than before in order to find the national security threat information they need.

The Government Argues that Section 702 is an Important Intelligence Tool

The NSA maintains that 702 surveillance "is the most significant tool in [the] NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world." [11] The IC cites 53 counterterrorism investigations in which information obtained under 702 "contributed in some degree to the success of the investigation" over the first five years of the program. [12] An independent panel established by President Obama, the Privacy and Civil Liberties Oversight Board, reached similar conclusions, stating in a 2014 report that "the information the [702] program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence." [13]

The effectiveness of 702 surveillance is perhaps most visible in the case of Najibullah Zazi, an Afghan-born American citizen who received bomb-making training in Pakistan and

planned to attack the New York City subway in September 2009. In a statement submitted to the House Judiciary Committee in February 2016, officials from the Office of the Director of National Intelligence, the Counterterrorism Division of the FBI, and the Signals Intelligence Directorate of the NSA claimed that, by using Section 702 authorities, the NSA was able to intercept discussions between Zazi and a foreign contact concerning the attack. These intercepted communications were then passed on to the FBI, which performed its own investigation which culminated in thwarting the attack and the arrest and conviction of Zazi. [14]

The case of Khalid Ouazzani and his co-conspirators, Sabirhan Hasanoff and Wesam El-Hanafi, is, according to former FBI Deputy Director Sean Joyce, another example of the effectiveness of 702 surveillance. Ouazzani, a U.S. citizen from Morocco, ran a used car parts store in Kansas City, Missouri, and provided material support to al-Qaeda by collaborating with Hasanoff and El-Hanafi. [15] Joyce indicated in testimony before the House Intelligence Committee that 702 surveillance tied Ouzzani to a Yemeni extremist, with this leading the FBI to investigate and eventually convict Ouazzani and his accomplices. [16]

Aside from these cases, the perception by terrorists that the U.S. is monitoring their communications could deter them from using communication technology to launch coordinated attacks. This deterrence could force terrorist groups to resort to the least deadly acts, like lone wolf attacks, to implement their agenda. It can also force them to rely upon in-person communications, with such communications likely being more susceptible to penetration by human intelligence sources.

While the government trumpets law enforcement successes under Section 702, it downplays the fact that such criminal investigations and prosecutions are carried out by the Justice Department and not the NSA. While the NSA gathers 702 information for the purpose of understanding national security concerns about foreigners abroad, the cases that the

government cites deal with U.S. persons, operating in the U.S., and prosecuted by the Justice Department, a domestic law enforcement body, subject to the Constitution and Fourth Amendment. And while the NSA is not constrained by the Constitution in its surveillance of non-U.S. persons outside the US, the Justice Department's job is to ensure that the Constitution is followed in the US.

Section 702's Drafters Overlooked How Law Enforcement Uses Intelligence Information

The Fourth Amendment of the U.S. Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Courts have interpreted this text as requiring government authorities seeking to perform searches to, absent certain exigent circumstances, (1) swear an affidavit (2) before a neutral, detached magistrate (3) setting out with particularity (i.e. specificity) (4) the place, person, or things to be searched or seized. Upon fulfilling these requirements, the judge before whom a law enforcement officer appears may choose to grant or deny that officer a search warrant, depending on whether the judge believes that there is probable cause that evidence of a crime will be found.

The Fourth Amendment's warrant requirements apply not only to physical searches, but also to searches of electronic information. Congress has explicitly acknowledged this in 18 U.S.C. § 2703 (the Stored Communications Act), which states that a "governmental entity may require the disclosure . . . of the contents of a wire or electronic communication . . . only pursuant to a warrant." Therefore, in a normal law enforcement context, a federal agent operating inside the

U.S. must adhere to the Fourth Amendment's warrant requirement when seeking to acquire and search an American's electronic communications.

While searches under the Stored Communications Act must be conducted pursuant to a warrant, with this offering assurances against unreasonable invasions of privacy, searches under Section 702 are noticeably lacking in such safeguards. This wouldn't be a problem if Section 702 databases only contained the information of non-U.S. persons. But Section 702, while targeted at non-U.S. persons, inevitably collects the information of U.S. persons as well. Indeed, the courts have said that the SCA applies inside the US, and that law enforcement officials cannot use that statute to compel companies to produce the information in the US. However, if such information transits the US, the government can collect it under Section 702, regardless of the location of the target.

When law enforcement officials examine Section 702 databases, they may search for "U.S. person identifiers" (terms or indicators that are linked to a U.S. person). No search warrant is required to query such information. Rather, a law enforcement official may search for this information if the search is "reasonably designed to 'find and extract' either 'foreign intelligence information' or 'evidence of a crime.'" [17] Further, although Section 702 imposes a low level of judicial scrutiny for the creation of the large pools of information in 702 databases, when law enforcement searches a database for a particular individual's communication, there is not higher judicial scrutiny for that query, despite the heightened privacy interest. In addition, for individual searches of 702 databases there is no neutral, detached magistrate; [18] sworn affidavit; or particularized statement. In fact, even if a court were engaged in overseeing individual searches of U.S. person identifiers, there would be no way for it to assess the reasonableness of an FBI officer's search, as the FBI does not require its analysts to document their rationales for querying U.S. person data.

While the standards for querying Section 702 data are well-suited for foreign intelligence purposes, they are woefully inadequate for law enforcement purposes. Under the Constitution, criminal defendants are entitled to protections from unreasonable searches and seizures, with the Fourth Amendment's Warrant Clause being the primary bulwark against such invasions of privacy. However, the broad discretion to collect information under Section 702 can be construed so as to allow law enforcement agencies, like the FBI, to access Section 702 data not just for foreign intelligence purposes, but for purposes that are wholly focused on domestic criminal prosecutions. Such access, which avoids the more exacting requirements of the Stored Communications Act, is often referred to as a "backdoor search" or "U.S. persons search," and there is significant evidence that such searches are a regular occurrence.

For example, in the Privacy and Civil Liberties Oversight Board's 2014 Report, the drafters noted that "[w]hen an FBI agent or analyst initiates a criminal assessment or begins a new criminal investigation related to any type of crime, it is routine practice . . . to conduct a query of FBI databases in order to determine whether they contain information on the subject of the assessment or investigation . . . The databases queried may include information collected . . . under Section 702." [19] The Board further noted that "many" FBI analysts and agents "who solely work on non–foreign intelligence crimes" query Section 702 databases.

The troubling nature of backdoor searches of Section 702 databases should not be downplayed. The warrant requirement is one of the foundations of the U.S.'s justice system. Without it, law enforcement is given a blank check to subject Americans to intrusive, unjustified invasions of private life. Backdoor searches are a refutation of the necessity of a warrant, a refutation that, gone unchallenged, could seriously undermine the Fourth Amendment protections guaranteed by the Constitution.

A practice that is just as troubling as the FBI's backdoor searches is the Justice Department's failure to notify criminal defendants when evidence is introduced against them that is derived from Section 702 surveillance. Section 702 requires the government to notify defendants whenever information obtained through 702 authorities will be used against them in criminal proceedings, [20] but there are indications that the government has often failed to fulfill such notice requirements. Most tellingly, for the first five years of collection under Section 702, not a single criminal defendant received notice of the use of evidence derived from its authorities, despite repeated testimony by government officials about the success of the program. [21] After this initial drought, DOJ issued five notices in the latter months of 2013 and the early months of 2014. [22] However, since April 2014, no further notices of the use of Section 702 data have been issued to criminal defendants. This suggests either a failure on the part of prosecutors to disclose the use of this information or that government officials are overstating the importance of this program in counterterrorism efforts.

Further, the failure to give notice to defendants about the use of Section 702-derived information prevents courts from reviewing the Constitutional adequacy of the surveillance statute, as applied in a law enforcement context.

Section 702's Drafters Overlooked Its Impact on U.S. Companies Operating Abroad

While the IC maintains that Section 702 has sufficient protections for U.S. persons operating abroad, there is a significant category of U.S. actors that have been adversely affected by U.S. overseas surveillance: U.S. technology companies trying to compete internationally.

When made aware of the extent of Section 702 surveillance by the Snowden revelations, foreign governments, concerned that dealing with U.S. telecom and tech companies could expose their data to U.S. surveillance, refused to renew their

contracts with U.S. companies and awarded contracts to foreign companies at the expense of their U.S. rivals. Examples of this may be found in Germany's 2014 refusal to renew a contract with Verizon for Internet services and Microsoft's 2013 loss of a contract to provide email services to the Brazilian government. [23] In addition to this loss of government contracts, U.S. companies lost consumers to foreign companies. For example, after the Snowden revelations a Norwegian email company, Runbox, which touts itself as a foreign alternative to U.S.-based email services like Gmail, benefited from a 34 percent annual increase in customers. [24] Some analysts estimate that NSA surveillance concerns could cost the U.S. cloud computing industry as much as $180 billion by 2016. [25]

Perhaps the most worrisome outgrowth of the Snowden revelations came in the European Court of Justice's (ECJ) decision to strike down the EU-U.S. Safe Harbor Agreement. The ECJ ruled that this pact, which allowed for U.S. companies to have their collection and use of EU persons' data classified as compliant with EU data protection laws, failed to comport with privacy standards set forth by Article 25(6) of EU Directive 95/46 and the EU's Charter of Fundamental Rights. The ECJ alluded to Section 702 programs when justifying its ruling, citing "legislation permitting the public authorities to have access on a generalised [sic] basis to the content of electronic communication" as one of the reasons for the Safe Harbor Agreement's invalidity. [26]

The invalidation of the Safe Harbor Agreement was no small matter. U.S. companies regularly transfer data about EU customers and employees across the Atlantic to their U.S.-based servers. [27] With the Safe Harbor gone, U.S. companies, absent standard contractual clauses or binding corporate rules, could now be forced to store consumer data in European facilities or be subject to penalties imposed by regulators. [28] The cost of localizing data or complying with each EU member's data protection regulations could be especially prohibitive for U.S. small and medium-sized enterprises. [29]

Although EU and U.S. officials have recently implemented a replacement for the Safe Harbor Agreement, a framework known as the EU-U.S. Privacy Shield, it is by no means certain that this successor agreement will withstand judicial scrutiny. In fact, less than three months after the Privacy Shield framework began to operate, the non-profit Digital Rights Ireland filed a challenge to it in the ECJ's lower General Court. [30] In its challenge, Digital Rights Ireland alleged that the European Commission's decision to approve the Privacy Shield did not comply with European law and cited Section 702 as a reason for such noncompliance. [31] The ECJ has yet to rule on this challenge.

One of the main objections that parties like Digital Rights Ireland have raised is that the EU-U.S. Privacy Shield still allows for generalized surveillance of EU communications. [32] Although, as part of the agreement, U.S. authorities assured European policymakers that "any access of public authorities to personal data will be subject to clear limitations, safeguards, and oversight mechanisms" and "affirm[ed] [the] absence of indiscriminate or mass surveillance," [33] the Europeans may be wise to be skeptical. In the past, even though U.S. authorities have assured Americans that their data is subject to certain protections, declassified FISC opinions and leaked documents reveal that such protections have often been flouted. If such disregard for the privacy interests of Americans has occurred, it is not outlandish to suspect that similar disregard will be expressed for Europeans' privacy interests.

Even if Privacy Shield withstands the scrutiny of the ECJ, there is no guarantee that the European Commission won't reassess its support for the program. Although U.S. officials have, with the impending advent of a Trump presidency, assured European authorities of the nation's continued commitment to surveillance limitations imposed through Privacy Shield, such assurances are only as good as the consistency with which they are applied by the incoming Administration.

The fragile nature of U.S. promises on Privacy Shield is highlighted by the stances of President-elect Trump's nominees for key national security positions. Trump's pick for CIA Director, Rep. Mike Pompeo, has been a prominent critic of efforts to reform U.S. surveillance practices and has accused the Obama Administration of "blunting its surveillance powers." [34] Trump's pick for Attorney General, Sen. Jeff Sessions, has been such an uncompromising cheerleader for surveillance that some worry that his tenure at the Justice Department could make "the Hoover era [look] like child's play." [35] If these surveillance reform skeptics walk back the protections offered to the Europeans, or worse, broaden the scope of U.S. surveillance, the European Commission may be reluctant to reauthorize Privacy Shield when it reviews the program in 2017. Such reluctance could portend future economic storms for the tech and telecom sectors, including the worrisome costs of data localization, punitive payouts in privacy-related litigation, and, in a worst-case scenario, the severance or severe curtailment of transatlantic data flows.

Section 702 Reforms Must Protect the Rights of Americans and Redefine Government's Relationship with U.S. Corporations

Section 702, while a helpful framework for conducting foreign intelligence, poses troubling quandaries when it comes to civil liberties and U.S. corporate interests. However, these worrisome conundrums can be addressed if lawmakers enact reforms that enhance the rights of Americans and redefine the government's relationship with U.S. corporations.

First, efforts should be made to address the backdoor searches and notice deficiencies evident in FBI use of Section 702 data. Although the FISC has deemed backdoor searches to be constitutional, many scholars believe that the FISC was wrong to classify them as such. For example, Amy Jeffress,

the former Counselor to the Attorney General for National Security and International Matters, argues that backdoor searches "are inconsistent with the requirements of the Fourth Amendment." [36] Georgetown law professor Laura Donahue claims that backdoor searches, among other practices facilitated by Section 702, have come at the cost of "inroads into rights that we have long – and for good reason – protected." [37] Making changes to Section 702 to address FBI queries using U.S. person identifiers and failures to give notice to criminal defendants would help ensure that Americans' constitutional rights are protected.

Second, efforts need to be made to redefine the government's relationship with the tech and telecom industries. Technology executives have repeatedly signaled their disapproval of what they describe as government overreach in the realm of surveillance. For example, in 2013 Facebook CEO Mark Zuckerberg said that "[r]eports about government surveillance have shown there is a real need for . . . new limits on how governments collect information." [38] Microsoft's general counsel Brad Smith went so far as to argue that government surveillance posed an existential risk to the American tech industry, arguing that "People won't use technology they don't trust. Governments have put this trust at risk." Statements such as these highlight the dissatisfaction that much of the tech industry currently has with the state of surveillance and drive home the need for the government to empower the industry to push back against surveillance practices that could harm companies' bottom lines. If such a rebalancing of government-industry relations is not prioritized, the government risks further antagonizing the industry and making it harder to work with tech companies to ensure the nation's security. Furthermore, the tech industry's unease with the current state of surveillance illustrates the need for lawmakers to seek out industry expertise when faced with making changes to Section 702, as any modifications can have a drastic impact on industry profitability and government relations with the tech industry.

Conclusion

Section 702 is a valuable intelligence tool that exhibits some significant deficiencies in its protections for U.S. persons in a law enforcement context and for U.S. competitive interests abroad. Policymakers should craft reforms that guard against the misuse of Section 702 by law enforcement and redefine the relationship between the IC and tech companies. As they do so, policymakers can ensure that Section 702 continues to fulfill its vital national security functions while also respecting the civil liberties and corporate interests of U.S. persons and companies.

TOPICS

NATIONAL SECURITY & POLITICS 82

END NOTES

1. The U.S. Intelligence Community is a group of 16 entities, both civilian and military, that gather information for governmental purposes. The members of the IC are: Air Force Intelligence, Army Intelligence, Marine Corps Intelligence, Navy Intelligence, Coast Guard Intelligence, the CIA, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the NSA, the FBI, the Department of Energy's Office of Intelligence and Counterintelligence, the Department of Homeland Security's Office of Intelligence and Analysis, the State Department's Bureau of Intelligence and Research, the Treasury Department's Office of Intelligence and Analysis, and the DEA's Office of National Security Intelligence. *See Members of the IC,* Office of the Director of National Intelligence, https://www.dni.gov/index.php/intelligence-community/members-of-the-ic#doe (last visited Jan. 23, 2017).

2. Offices of Inspectors Gen. of the Dep't of Def., Dep't of Justice, Cent. Intel. Agency, Nat'l Sec. Agency, and Office of the Dir. of Nat'l Intel., 2009-0013-A, Report on the President's Surveillance Program (July 10, 2009), http://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html.

3. *Id.* at 7-8.

4. The Snowden leaks revealed a number of U.S. companies that supposedly give content to the DITU and NSA. Among them are Google, Facebook, Yahoo!, Skype, Apple, AOL, Microsoft, and PalTalk. *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps into user data of Apple, Google and others*, Guardian, June 7, 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

5. *See* 50 U.S.C. § 1881a(h) (2016).

6. Shane Harris, *Meet the Spies Doing the NSA's Dirty Work*, Foreign Policy, Nov. 21, 2013, http://foreignpolicy.com/2013/11/21/meet-the-spies-doing-the-nsas-dirty-work/.

7. Mieke Eoyang, *Beyond Privacy & Security: The Role of the Telecommunications Industry in Electronic Surveillance*, Hoover Working Group on National Security, Technology, and Law, Apr. 8, 2016, https://www.lawfareblog.com/beyond-privacy-and-security-role-telecommunications-industry-electronic-surveillance.

8. Nat'l Sec. Agency, Special Source Operations, SSO Corporate Portfolio Overview, at 5 (Jan. 8, 2007), https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01a5/f29cea54.dir/doc.pdf.

9. Ashley Gorski & Patrick C. Toomey, *Unprecedented and Unlawful: The NSA's "Upstream" Surveillance*, Just Security, Sept. 19, 2016, https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-surveillance/.

10. Privacy & Civil Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 33-37 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf#page=42.

11. President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World, at 143 (Dec. 12, 2013), https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world.

12. *Id.* at 144-45. *But see* Bailey Cahall, Peter Bergen, David Sterman, & Emily Schneider, *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, New America Foundation, Jan. 13, 2014, https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/ (arguing that 702 surveillance has played a minimal role in the investigation and prosecution of terrorism cases).

13. Privacy & Civil Liberties Oversight Bd., *supra* note 9, at 2.

14. Marshall Erwin, *Connecting the Dots: Analysis of the Effectiveness of Bulk Phone Records Collection*, Hoover Institution, Jan. 13, 2014, https://www.justsecurity.org/5605/guest-post-connecting-dots/; *see also* Matt Apuzzo & Adam Goldman, Enemies Within: Inside the NYPD's Secret Spying Unit and bin Laden's Final Plot Against America, 8-9, 273-74 (2013).

15. Plea Agreement, U.S. v. Khalid Ouazzani, No. 10-00025-01-CR-W-HFS (W.D. Mo. May 19, 2010), http://www.investigativeproject.org/documents/case_docs/2236.pdf.

16. Cahall et al., *supra* note 11.

17. Memorandum Opinion and Order, *In re* [REDACTED], No. [REDACTED], at 26-27, (FISA Ct. Nov. 6, 2015),https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf [hereinafter Hogan Memorandum Opinion].

18. Although the FISC does approve the IC's targeting and minimization procedures, it has no role in approving individual queries of U.S. person information.

19. Privacy & Civil Liberties Oversight Bd., *supra* note 9, at 137.

20. 50 U.S.C. § 1881(e), 1806.

21. Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance – Again?*, Just Security, Dec. 11, 2015, https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/.

22. *Id.*

23. Andrea Peterson, *German government to drop Verizon over NSA spying fears*, Wash. Post, June 26, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/06/26/german-government-to-drop-verizon-over-nsa-spying-fears/ ; *Brazil to create its own email system after protesting U.S. spying*, UPI, October 14, 2013, http://www.upi.com/Brazil-to-create-its-own-email-system-after-protesting-US-spying/69911381785172/.

24. Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. Times, March 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

25. James Staten, *The Cost of PRISM Will Be Larger Than ITIF Projects*, Forrester Research, Aug. 14, 2013, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

26. Case C-362/14, *Schrems v. Data Protection Comm'r*, 2015 E.C.R. 650.

27. Joshua P. Meltzer, *Examining the EU safe harbor decision and impacts for transatlantic data flows*, Brookings Institution, Nov. 3, 2015, https://www.brookings.edu/testimonies/examining-the-eu-safe-harbor-decision-and-impacts-for-transatlantic-data-flows/.

28. *See* Sam Schechner, *Firms Weigh Moving Data From U.S. to Europe*, Wall St. J., Nov. 2, 2015, http://www.wsj.com/articles/firms-shift-data-to-europe-as-safe-harbor-pact-ends-1446478648.

29. Matthias Bauer, Fredrik Erixon, Michal Krol & Hosuk Lee-Makiyama, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, European Centre for International Political Economy, March 2013, https://www.uschamber.com/economic-importance-getting-data-protection-right.

30. Case T-670/16, *Digital Rights Ireland v. Comm'n*, 2016 E.C.R. _____, http://curia.europa.eu/juris/document/document.jsf?text=&docid=185146&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=474396.

31. Id.

32. Id.

33. *EU-U.S. Privacy Shield*, European Commission, July 2016, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf.

34. Mike Pompeo & David B. Rivkin, Jr., *Time for a Rigorous National Debate About Surveillance*, The Wall St. J., Jan. 3, 2016, http://www.wsj.com/articles/time-for-a-rigorous-national-debate-about-surveillance-1451856106.

35. Issie Lapowsky & Andy Greenberg, *Jeff Sessions' Nomination as Attorney General Alarms Civil Libertarians*, Wired, Nov. 18, 2016, https://www.wired.com/2016/11/jeff-sessions-nomination-attorney-general-alarms-civil-libertarians/.

36. Hogan Memorandum Opinion at 39.

37. Laura K. Donohue, The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age 74 (2016).

38. *Global Government Surveillance Reform*, Reform Government Surveillance, https://www.reformgovernmentsurveillance.com/ (last visited Jan. 24, 2017).