THIRD WAY

REPORT *Published March 19, 2015 • 12 minute read*

Restoring Trust between U.S. Companies and Their Government on Surveillance Issues

Mieke Eoyang
Vice President for the National Security Program
@MiekeEoyang

Chrissy Bishai
Fellow, National Security Program

Allegations of intrusive U.S. government electronic surveillance activities have raised international outcry and created antagonism between U.S. technology companies and the government. Without a bold and enduring reform, American companies will continue to suffer a competitive disadvantage from perceptions of U.S. government intrusion into their data. We propose bringing electronic surveillance collection from U.S. companies into an existing statutory framework in order to reassure international customers and to respect the rights of U.S. companies operating abroad.

The Problem

In the wake of the Snowden revelations, people around the world have become uneasy about the security of their communications that flow through the servers of American companies. [1] They now fear—not without reason—that the NSA has broad access to a wide range of their data that may not have any direct relevance to the core foreign policy or security concerns of the United States. [2]

Snowden has also alleged that the NSA accessed American companies' data without their knowledge. [3] American technology companies reacted with outrage to media reports that, unbeknownst to them, the U.S. government had intruded onto their networks overseas and spoofed their web pages or products. [4] These stories suggested that the government created and snuck through back doors to take the data rather than come through well-established front doors. [5]

Beyond the broad implications for civil liberties and diplomacy, these fears led to two immediate consequences for the industry: First, many U.S. companies shifted to an adversarial relationship with their own government. They

moved to secure and encrypt their data to protect the privacy rights of their customers. [6] They are pushing for reform. [7] They are building state-of-the-art data centers in Europe and staffing their high-paying jobs with Europeans, not Americans. [8] They are challenging the government in court. [9]

Second, international customers of U.S. technology and communications companies began taking their business elsewhere. Brazil decided against a $4.5 billion Boeing deal and cancelled Microsoft contracts. [10] Germany dropped Verizon in favor of Deutsche Telekom. [11] Both of these examples suggest that if even friendly governments can go to the expense and trouble of dropping American companies, foreign individual and corporate customers could certainly decide to switch their data providers for greater privacy protection. Simply put, the reputational harm had a direct impact on American companies' competitiveness—some estimate that it has cost U.S. tech firms $180 billion thus far. [12]

Defenders of the programs may argue that the Snowden allegations are overblown or that foreign companies are just using the revelations for their own protectionist purposes. But it doesn't matter if the allegations are actually true because the global public believes them to be true, and they are therefore real in their consequences.

In many ways, the Snowden revelations have created a sense of betrayal among American companies. Some had been providing information to the NSA through existing legislative means – either under Section 215 of the USA Patriot Act, [13] or under Section 702 of the FISA Amendments Act (FAA). [14] It was unsettling to read stories that, outside of this statutorily compelled cooperation, the government had been getting access to huge amounts of their data in other unauthorized ways. As one tech employee said, "the back door makes a mockery of the front door."

Fixing the Problem Means Changing the Existing Legal Framework

Currently, the U.S. collects electronic communications under four main authorities.

Authority	Section 215 of the USA Patriot Act	Section 702 of the FISA Amendments Act	FISA	Executive Order 12333
Scope	Wholly domestic communications	One end domestic	Domestic	Foreign-to-foreign communications [may include U.S. persons who are abroad]
Kind	Metadata	Content	Any	Any
Usage	For an authorized investigation. . . to protect against int'l terrorism or clandestine action	Foreign intelligence	"Necessary" to protect against hostile acts.	Foreign Intelligence

For collection occurring under both 215 and 702, the companies would have been served with an order compelling production of their data. But outside the U.S., Executive Order 12333, [15] the long-standing guidance for foreign intelligence activities, would govern the kind of collection that has caused international outrage.

E.O. 12333, signed by President Reagan, set the ground rules and authorization for foreign intelligence collection when the nation's primary security threat was the Soviet Union. At that time, traditional intelligence activities would have been focused on other nation-states—identifying their spies, trying to recruit spies for the U.S., and trying to steal other countries' secrets while protecting our own. But the growth of terrorist groups' capabilities, and particularly the 9/11 attacks, helped dissolve the separation between traditional overseas espionage and counter-terrorism.

As the nation was grappling with new threats posed by terrorism, people around the world were sharing more and more of their information online and using mostly American companies to do so. Yet the legal framework that had once recognized privacy rights was ill-suited to the Internet Age. The Intelligence Community's traditional position that constitutional rights like the Fourth Amendment's privacy protections didn't apply to non-Americans outside the U.S. might have been clear when travelling and communicating internationally were more difficult. But today's free-flowing movement of people and data means that the "nationality" of an individual's communications is far less obvious. [16]

While extending constitutional or privacy protections to foreigners abroad is a tricky legal proposition, for many their data is being held by entities that *are* entitled to the due process and privacy protections of the U.S. Constitution: American companies. Our tech firms often act as custodians of other people's data, and as such don't have the same heightened privacy interests as the targets of that data. But accessing the companies' data without even giving notice to the owner of the servers raises serious constitutional questions.

As a politician once famously noted, "corporations are people too." [17] As a legal (if not political) matter, he was right—these American tech companies are "U.S. Persons," and they therefore should know when the government seeks to access the data they possess. The companies should be entitled to notice, especially since they can be compelled to cooperate with law enforcement requests to hand over user data. Those protections should hold true regardless of whether the user data sought by the U.S. government is that of Americans or non-Americans.

In addition to those privacy protections that all U.S. persons enjoy under the Constitution, both at home and abroad, surveillance reform should meet the following principles when dealing with information about or from Americans:

- The U.S. government should have a process, consistent with the Constitution, to acquire from companies the information that it needs to secure the country.
- The U.S. government should have a national security reason to collect the information that it requests.
- U.S. companies should not have to fear unauthorized access to their data or products from their own government.
- Any process to acquire information from U.S. companies should have safeguards to prevent misuse or intentional over-collection.

The Solution

Include Overseas Collection from American Companies in Existing Statutory Frameworks

In order to meet the principles above, we propose that FAA's 702 framework be the exclusive means for conducting electronic surveillance when the information is in the custody of an American company ("FAA Exclusivity"). Section 702 of FAA provides procedures to authorize data collection of *foreign targets* reasonably believed *to be outside the U.S.* It empowers the Attorney General (AG) and Director of National Intelligence (DNI) to jointly certify a high volume of targeting and does not require the requesters to identify specific non-U.S. persons who will be targeted. Under this 702 framework, information on foreigners that's in the custody of a U.S. company should be subject to the following rules:

1. The data must relate to targets "reasonably believed" to be outside the U.S. (can include foreign persons, governments or their factions and similar entities).

2. The AG and DNI must jointly submit annual "certifications" to the Foreign Intelligence Surveillance Court (FISC).

3. Certifications must identify categories of foreign intelligence targets that the Government wants to surveil electronically; they do not need to identify specific persons to be targeted.

4. Certifications may include information or representations from other federal agencies authorized to cooperate with the AG, DNI, or Director of the NSA.

5. Certifications must be reviewed by the FISC, which can authorize the targeting if they deem that the statutory requirements have been met.

6. After the certifications are approved, the AG and DNI issue (written) “directives” to the providers, ordering them to assist the government.

7. Collection should be executed with the appropriate “minimization procedures” in place to limit the acquisition, retention, and dissemination of any non–publicly available U.S. person information acquired through the Section 702 program.

8. The AG, in consultation with the DNI, must adopt FISC-approved targeting and minimization procedures that are “reasonably designed” to ensure that the Government does not collect wholly domestic communications, and that only persons outside the U.S. are surveilled.

9. The AG and DNI must also create acquisition guidelines (which are not subject to FISC approval).

Advantages of an FAA Framework

Shifting the legal authority for collection of data in the custody of an American company from E.O. 12333 to an FAA framework would have a number of advantages. Most importantly, it would create a way for the government to get the data it needs from American companies while giving those firms assurances that their data would not be accessed in other unauthorized ways. In particular, the FAA framework would create specific purposes for which the information could be sought, rather than allow the indiscriminate scooping up of every aspect of a person’s communications. FAA’s stated purpose is to acquire foreign intelligence information, which it defines as "information that relates to the ability of the U.S. to protect against an actual or potential attack by a foreign power; sabotage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine intelligence activities by a foreign power."

The FAA framework would also create a requirement that the Executive Branch explain how the information sought meets the statutory purposes. And there would be the additional check of an independent judge who would review the certifications and issue directives. Though this process is *ex parte*, and therefore a potential rubber stamp for the government, there have been no documented instances of intentional abuses of the system in seeking information beyond the statutory purposes.

Finally, the FAA framework would subject information sought from U.S. companies to the statutory oversight requirements of the law. These are extensive and explicit. [18]

In addition to FAA's inherent protections, FAA Exclusivity would send a powerful message to the rest of the world: when the U.S. conducts electronic surveillance overseas from American companies, it is doing so for a particular national security purpose. The FAA structure with FISC review provides an independent check that the statutory purposes are met. Through transparency agreements with the government, the American companies would be able to provide their customers with some sense of how many requests are made.

FAA Exclusivity would not change the E.O. 12333 authorities with respect to non-U.S. companies. It would not change E.O. 12333 authorities when the Executive Branch seeks to obtain the information in some way other than through a U.S. company that holds the data (i.e. traditional espionage, like breaking into a target's laptop, parking a surveillance van outside their house, or sending a spy, would still be permissible).

Of course, FAA Exclusivity wouldn't solve every problem. It would not prevent foreign governments from collecting information themselves and then providing it to U.S. intelligence agencies, as U.S. law cannot bind a foreign government. And some may argue that FAA provides inadequate civil liberties protections for Americans. This proposal says nothing about the adequacy of that statute in this respect. What it says is that for data held by an American

company about a target that is not a U.S. person, the checks within FAA are stronger than those solely under E.O. 12333.

Others have argued that the FAA shifts the burden of cooperation solely onto the company, which will suffer greater reputational harm as a more witting participant in affirmatively granting the government's requests. However, companies have suffered reputational harm as a result of allegations of unwitting cooperation. Making the cooperation known, even if it's secret, gives the companies the opportunity to account for it in their own planning.

The move by certain U.S. companies to place subsidiaries in foreign ownership to resist requests by the U.S. government presents an interesting twist on this idea. In shifting the balance back to increased protections for U.S. companies, this legislation would change the incentives so that claiming U.S. law would have operational advantages in giving companies uniformity of law for all their data. This would also encourage the use of a single choice of law for all data governed by a company—that of the nationality of incorporation—rather than encouraging a choice of law patchwork to govern the data as it flows around the world.

Finally, some foreign multinational companies operating in the U.S. and abroad may argue that this is inconsistent with principles that we treat all companies operating in the U.S. the same way for purposes of law. While that would remain true under this proposal, it would create a difference in how the U.S. treats U.S. companies operating *abroad* compared to how it treats foreign companies abroad. But stretching the U.S. Constitution to foreign companies abroad is to stretch the document too far. If, on the other hand, those companies see advantage in changing their nationality to U.S. in order to claim protections of those laws, then that is the corporate version of the kind of immigration patterns that America has seen since its founding.

Conclusion

Using FAA's framework as the exclusive means to access data that U.S. companies are holding will give the Intelligence Community a statutory framework to be able to get the intelligence information that it needs to protect the nation while restoring the trust relationship between the companies and our government. In addition, it will help restore the faith of foreign governments and customers that when American companies are acting overseas, they bring with them American values, including those of privacy protections.

TOPICS

NATIONAL SECURITY & POLITICS 82

END NOTES

1. Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 6, 2013. Accessed March 16, 2015. Available at: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; See also Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *The Washington Post*, June 7, 2013. Accessed March 16, 2015. Available at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; See also Barton Gellman, Aaron Blake and Greg Miller, "Edward Snowden comes forward as source of NSA leaks," *The Washington Post*, June 9, 2013. Accessed March 16, 2015. Available at: http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html

2. United States, Office of the Director of National Intelligence, "DNI Clapper Declassifies and Releases Telephone Metadata Collection Documents," Press Release, July 31, 2013. Accessed March 16, 2015. Available at: http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/908-dni-clapper-declassifies-and-releases-telephone-metadata-collection-documents.

3. Laura Poitras, Marcel Rosenbach, Fidelius Schmid, Holger Stark and Jonathan Stock, "How the NSA Targets Germany and Europe," *Der Spiegel,* July 1, 2013. Accessed March 16, 2015. Available at: http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html.

4. Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers in this respecta person's er this directly to be on record. worldwide, Snowden documents say," *The Washington Post,* October 30, 2013. Accessed March 4, 2015. Available at: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

5. Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post,* October 30, 2013. Accessed March 4, 2015. Available at: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

6. BBC Technology, "Yahoo to encrypt all users' personal data," *British Broadcasting Corporation*, November 19, 2013. Accessed March 4, 2015. Available at: http://www.bbc.com/news/technology-25001373; Craig Timberg, "Newest Androids will join iPhones in offering default encryption, blocking police," *The Washington Post*, September 18, 2014. Accessed March 4, 2015. Available at: http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/

7. "The Principles," *Reform Government Surveillance* [Coalition]. Accessed March 4, 2015. Available at: https://www.reformgovernmentsurveillance.com/.

8. Paul McDougall, "Why Are Apple, Amazon Data Center Jobs Going To Europe? Blame The NSA," *The International Business Times*, February 26, 2015. Accessed March 4, 2015. Available at: http://www.ibtimes.com/why-are-apple-amazon-data-center-jobs-going-europe-blame-nsa-1829260.

9. Ewen MacAskill, "Yahoo files lawsuit against NSA over user data requests," *The Guardian*, September 9, 2013. Accessed March 16, 2015. Available at: http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests; See also *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*, 13 Mag. 2814, United States District Court, Southern District of New York, April 25, 2014, Accessed March 16, 2015. Available at: http://pdfserver.amlaw.com/nlj/microsoft-warrant-sdny.pdf; See also "Amicus Contributors, Microsoft's Case Challenging a U.S. Search Warrant," Microsoft Corporation, Memo, December 15, 2014. Accessed March 16, 2015. Available at: http://mscorp.blob.core.windows.net/mscorpmedia/2014/12/Amicus-Briefing-Filers_Supporters.pdf.

10. Claire Caine Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *The New York Times*, March 21, 2014. Accessed March 4, 2015. Available at: http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

11. Alexandra Hudson, "German government cancels Verizon contract in wake of U.S. spying row," *Reuters*, June 26, 2014. Accessed March 4, 2015. Available at: http://www.reuters.com/article/2014/06/26/us-germany-security-verizon-idUSKBN0F11WJ20140626.

12. Salvador Rodriguez, "NSA 'Equation' Fallout: Experts Say Damage To US Tech Firms Could Top $180B" *The International Business Times*, February 17, 2015. Accessed March 4, 2015. Available at: http://www.ibtimes.com/nsa-equation-fallout-experts-say-damage-us-tech-firms-could-top-180b-1819264.

13. 50 USC Secs., 1861-2, 2008. Accessed March 16, 2015. Available at: http://www.gpo.gov/fdsys/granule/USCODE-2009-title50/USCODE-2009-title50-chap36-subchapIV-sec1861.

14. 50 USC Sec., 1801, 2008. Accessed March 16, 2015. Available at: http://www.intelligence.senate.gov/laws/pl110261.pdf; See also United States, Congress, House, "FISA Amendments Act Reauthorization Act of 2012," Pub. L. No. 112-238, 126 Stat. 1631, 2012. Accessed March 16, 2015. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-112publ238/pdf/PLAW-112publ238.pdf.

15. 46 Fed. Reg. 59941, 1981. Accessed March 16, 2015. Available at: http://www.archives.gov/federal-register/codification/executive-order/12333.html

16. See generally, "The Un-Territoriality of Data" by Jennifer Daskal, *Yale Law Review*, forthcoming.

17. Philip Rucker, "Mitt Romney says 'corporations are people,'" *The Washington Post*, August 11, 2011. Accessed March 4, 2015. Available at: http://www.washingtonpost.com/politics/mitt-romney-says-corporations-are-people/2011/08/11/gIQABwZ38I_story.html.

18. Section 702 of the FISA Amendments Act includes a wide variety of oversight mechanisms, including:

a) The judicial review provided by the FISC (described above).

b) Every six months the AG and DNI must provide Congress and FISC with an assessment of compliance with the targeting and minimization procedures, in addition to compliance with the acquisition guidelines.

c) The head of each branch of the IC that is conducting authorized 702 acquisitions must oversee an annual review of surveillance implementation.

d) At least once every 60 days, Department of Justice attorneys must coordinate with the Office of the Director of National Intelligence (ODNI) to conduct on-site reviews of IC agencies that are using 702 surveillance. (These reviews include routine examinations of the agencies' targeting determinations).

e) The Inspector General of the Department of Justice and the inspector general of each IC agency authorized to collect under 702 are permitted to review certain elements of the implementation.