THIRD WAY

MEMO *Published May 10, 2016 • 9 minute read*

Statement for the Record: Beyond Privacy & Security: The Role of the Telecommunications Industry in Electronic and Surveillance

Mieke Eoyang
Vice President for the National Security Program
@MiekeEoyang

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

By Mieke Eoyang
Vice President for the National Security Program, Third Way

Published by Lawfare on April 11, 2016

Available at: https://www.lawfareblog.com/beyond-privacy-security-role-telecommunications-industry-electronic-surveillance-0

As the sunset of the FISA Amendments Act approaches, Congress must determine whether the legislation should be reauthorized as is, reformed, or allowed to sunset. In deciding, the debate is often framed as a balance between government power and individual privacy. Frequently overlooked is the critical role of the communications companies, who as physical and legal gatekeepers regulate government access to private information. This testimony is an excerpt of a longer paper [1] that examines this gatekeeper

function and recommends surveillance reforms that will reinforce it, without denying necessary government access to information.

In particular, the paper argues, Congress has an opportunity to use the next renewal of the FISA Amendments Act (FAA) to review the safeguards in the statute and address the concerns raised by American technology companies in the wake of Edward Snowden. Allegations that the NSA accessed the overseas, internal networks of U.S. companies in secret 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. [2] Stories describing how the U.S. government collects data in bulk spooked overseas consumers and companies, particularly in Europe and South America, who began cancelling contracts with American companies and turning to foreign providers. [3]

European regulators have begun scrutinizing the relationship between U.S. companies and intelligence agencies, transforming consumer discontent abroad into a potentially distressing legal obstacle to cross-border data flows. This situation has led many U.S. technology companies to assume an adversarial stance vis-à-vis their own government, who they and their foreign customers perceive to be overbroad in its approach.

When it comes to designing foreign intelligence collection, many national security professionals question the relevance of industry preferences. But there are important reasons to account for these concerns. The growing Internet economy and the technology firms that run it are an essential part of the American economy. Encouraging growth and American competitiveness in foreign markets is a bedrock principle of U.S. economic policy. American Internet technology dominates the global market and proliferates freedom of expression, freedom to organize, and a diversity of opinion.

More specifically, it is in the interest of the Intelligence Community to respect industry's perspective. If the

government treats the companies as just another surveillance target to exploit, business leaders will view the government as yet another unauthorized user to keep out. That kind of rivalry frustrates the government's legitimate interest in accessing information necessary to securing the nation. The FBI's recent attempt to compel Apple to break its own security measures has only fanned those flames. It's time to turn down the temperature.

In approaching surveillance reform from the perspective of private industry, Congress should consider three proposals to fix these problems: (1) extending the FAA to apply to all overseas intelligence collection *sourced from a U.S. corporation*; (2) amending the FAA to clarify that U.S. companies must filter data using court-authorized selectors *before* handing it over to government agencies; and (3) funding the establishment of an international working group to harmonize standards on electronic surveillance.

FISA Exclusivity

First, the U.S. government must placate American companies enraged by allegations that the NSA secretly accessed their data and modified their products. The best way to do this is to expand the FAA framework to cover *all* overseas intelligence collection that draws from a U.S. corporate source. The FAA would become the *exclusive means* for obtaining data from U.S. companies in order to conduct electronic surveillance.

Specifically, Congress could mandate that: (1) whenever the government wants overseas data on non-U.S. persons reasonably believed to be outside the United States, (2) which is in the possession of or transmitted by a U.S. company, (3) agencies shall only compel production of that data using a FISC order provided to the company. Surreptitious collection against U.S. corporations would be banned. Executive Order 12333 (EO 12333) could no longer authorize the clandestine collection of data held within the networks of U.S. companies, even if the interception occurred outside of U.S. territory.

This would leave the IC free to target, using EO 12333, the information of foreign individuals held by foreign entities. 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 U.S. persons based on probable cause.

FAA exclusivity would reassure companies that court authorization was the only avenue by which the US government intentionally accesses *their* infrastructure worldwide, restoring a sense of forthrightness in the presently-strained relationship. Further, the U.S. technology industry could turn to their foreign customers and users and point to the FAA as a high standard affording judicial review and congressional oversight—something other governments do not offer in the context of foreign intelligence collection. Transparency reporting structures agreed to between the companies and the government—not feasible under EO 12333—would give international customers and users some sense of how small a proportion of the total traffic was requested.

Reassuring Foreign Customers

A hotly debated question at the heart of the post-Snowden debate is at what point government surveillance constitutes a privacy violation. Are individual rights implicated when the government copies electronic data, filters the data for potentially useful information, searches the post-filter data, or stores the filtered data? According to the Privacy and Civil Liberties Oversight Board (PCLOB), Section 702 of the FAA authorizes so-called "Upstream" surveillance, by which the NSA accesses Internet data via "backbone" fiber optic cables. It then runs the data through two electronic filters, the first of which removes any purely domestic communications. The second filter eliminates any communications that do not contain an authorized "selector," such as an email address. The remaining data "take" comprises only those communications containing selectors, and is held by the NSA for review, analysis, and dissemination (subject to certain

restrictions). Congress should amend the FAA to clarify that government agencies must provide these filters to private companies, who would themselves sift the backbone data and deliver the filtered product to the government. The government would compensate industry for these added costs. Affirming the custody of the handover interface could resolve numerous privacy concerns by those who fear the government is collecting data in bulk. It would eliminate the possibility that the government might abuse its position and use bulk data in improper ways—no matter how strong the legal 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. With this reform, 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.

Such a change is not politically impossible. It would mirror similar reforms to domestic metadata collection made by the USA FREEDOM Act. The government would retain access to important foreign intelligence information. Considering the administration's public position that the NSA only accesses post-filter data, it would be hard-pressed to criticize the transfer of the handover interface into private

International Surveillance Working Group

Going forward, this will not be the last challenge to electronic surveillance norms, and the international community must at least try to find a lasting solution. We are in the middle of a golden age of surveillance where governments can compel production of location data, browser histories, message drafts, private online diaries, as well as content and metadata around calls. Governments cannot assume their surveillance programs will remain secret forever, and thus must design them keeping in mind the consequences of public disclosure. For obvious reasons, there is little discussion around the state of global norms around national security espionage. The U.S. should jumpstart an international forum 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 U.S. business abroad and U.S. diplomatic relations with our allies. To be able to discuss the national security implications in light of the economic impacts, the U.S. should start a NATO-OECD working group to discuss international norms around privacy, security, and trans-border data flows. This would allow the U.S. and Europe (and some non-European allies) to begin to talk about electronic surveillance norms and have both the 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 consider industry concerns, both to ensure future cooperation, and to protect U.S. competitiveness abroad. The U.S. government must rectify the current relationship with technology companies, poisoned by allegations that the NSA obtained unauthorized access to their data and/or products. Demonstrating a respect for U.S. corporate integrity by acquiring information through court process, rather than breaking in, could reduce corporate opposition. In order to protect U.S. competitiveness abroad, the U.S. could end bulk, unfiltered foreign collection in favor of a system that keeps the unfiltered stream in the private sectors' hands, restricting government access to only the information necessary to protect national security. And, finally, we must begin a conversation around electronic surveillance norms with our closest allies, establishing a forum to discuss economic and security considerations and develop balanced solutions.

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

TOPICS

NATIONAL SECURITY & POLITICS 82

END NOTES

1. Mieke Eoyang, Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance, Aegis Paper Series No. 1603 (Hoover Institution, 2016), *available at* https://lawfare.s3-us-west-2.amazonaws.com/staging/2016/307155829-Beyond-Privacy-and-Security-The-Role-of-the-Telecommunications-Industry-in-Electronic-Surveillance-by-Mieke-Eoyang.pdf.

2. *See, e.g.*, Daniel Thomas, *Cisco boss calls on Obama to rein in surveillance*, Financial Times, May 18, 2014, https://next.ft.com/content/a697c292-de80-11e3-9640-00144feabdc0?__i__location=http://www.ft.com/cms/s/0/a697c292-de80-11e3-9640-00144feabdc0.html; Sean Gallagher, *Googlers say "F*** you" to NSA, company encrypts internal network*, ArsTechnica, Nov. 6, 2013, http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/; Barton Gellman, Ashkan Soltani, and Andrea Peterson, *How we know the NSA had access to internal Google and Yahoo cloud data*, Wash. Post, Nov. 4. 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/.

3. *See, e.g.*, David McCabe, *Study: Surveillance will cost US tech sector more than $35B by 2016*, The Hill, June 9, 2015, http://thehill.com/policy/technology/244403-study-surveillance-will-cost-us-tech-sector-over-35b-by-2016; *German government cancels Verizon contract in wake of U.S. spying row*, Reuters, June 26, 2014, http://www.reuters.com/article/us-germany-security-verizon-idUSKBN0F11WJ20140626; Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. Times, Mar. 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.