Surveillance’s Future: A Pragmatic Take from the Center for a New American Security

Peter Margulies
Roger Williams University School of Law

Follow this and additional works at: https://docs.rwu.edu/law_fac_fs

Part of the National Security Law Commons

Recommended Citation

This Article is brought to you for free and open access by the Law Faculty Scholarship at DOCS@RWU. It has been accepted for inclusion in Law Faculty Scholarship by an authorized administrator of DOCS@RWU. For more information, please contact mwu@rwu.edu.
SURVEILLANCE

Surveillance’s Future: A Pragmatic Take from the Center for a New American Security

By Peter Margulies  Monday, December 12, 2016, 2:08 PM

Privacy Paradox: Rethinking Solitude

The 2016 election has sharpened debate around the reauthorization of Section 702 of the FISA Amendments Act of 2008, which will sunset in 2017. A new report by the Center for a New American Security (CNAS) offers balanced guidance on 702 and other issues at the intersection of surveillance, security, economics, and privacy. The new report is essential reading because it suggests concrete reforms in Section 702, while arguing for retention of key components of a program that independent entities like the Privacy and Civil Liberties Oversight Board and the President’s Review Commission have agreed provides the U.S. with valuable intelligence.

The report, co-authored by CNAS CEO Michele Flournoy and Senior Fellow Adam Klein, rejects the common trope of surveillance policy as a zero-sum game between security and privacy. The report notes that privacy safeguards can bolster the standing of U.S. technology firms—which took a bruising in the wake of Edward Snowden’s disclosures—and therefore build on the United States’ traditional technological strengths. Similarly, while surveillance can intrude on privacy, it can also preserve it, as David Pozen writes here, by supplying tools to combat cyber criminals who harvest personal information to serve their own agendas. Rightly conceived, privacy and security are complementary.

This preference for solutions over sloganeering typifies the CNAS report’s suggestions for reform of Section 702, under which the Foreign Intelligence Surveillance Court (FISC) approves procedures likely to return foreign intelligence information from communications in which one party is reasonably believed to be located outside the United States. Take the important issue of whether intelligence and law enforcement agencies should be able to use U.S. person queries on data incidentally collected under 702, even though the government cannot target any U.S. person under the statute. While some privacy advocates have argued that Congress should require that officials obtain a court order for all such queries (see the Brennan Center’s report here), the CNAS authors take a more balanced view.

CNAS suggests that law enforcement agencies explain why the capacity to pose U.S. person queries of content from the tailored PRISM program is essential. Government would also explain why access to metadata such as phone records would be insufficient. (The debate here is only about the PRISM program; the government has long prohibited queries of the Upstream program which collects data at internet hubs, since limits in current technology mean that Upstream collection inevitably results in incidental collection of wholly irrelevant U.S. person data, which is then minimized by the NSA.)

As I suggest in a recent paper on 702 reauthorization here, the government can readily explain why barring U.S. person queries of PRISM data would pose a risk to security. Connecting the dots in far-flung terror investigations requires quick reactions. Those reactions would be stymied by the 72-plus hours necessary to obtain a court order. Even an exigent circumstances exception to a court-order requirement, like one recommended by former PCLOB chair David Medine here, would hobble counterterrorism efforts. Often the government will not know until the last minute that a risk has ripened into an imminent threat. Insisting on proof of exigency will give groups like ISIS room to maneuver. As CNAS urges, government agencies such as the FBI should make that case to Congress, which should reauthorize Section 702 without the added burden to law enforcement of obtaining a court order for U.S. person queries of PRISM data.

While the CNAS report urges Congress not to impose undue hindrances on surveillance, the report also warns against legislative interference with accountability mechanisms such as the PCLOB (see PCLOB board member Rachel Brand’s discussion of intelligence oversight here). The Fiscal Year 2017 Intelligence Reauthorization Act would hamper the PCLOB’s performance of its watchdog role, by expressly confining PCLOB oversight to the “privacy and civil liberties of United States persons.” As CNAS observes, this restriction would send a counterproductive message to the EU, by suggesting that there are no checks on U.S. surveillance abroad. President Obama’s landmark Presidential Policy Directive No. 28 (PPD-28), issued in January 2014, aimed to counter that impression, which had become widespread abroad after Snowden’s revelations. PPD-28 stated forthrightly that the U.S. strove to respect the privacy rights of all people around the world. The bill CNAS criticizes would undermine the good will that PPD-28 has generated, and exacerbate the trust deficit that Snowden triggered among our allies.

When it comes to the trust deficit regarding U.S. surveillance internationally, exhibit A is the decision of the Court of Justice of the European Union (CJEU) in Schrems v. Data Protection Commissioner. The CNAS report expertly dissects Schrems, which invoked an incomplete and out-of-date account of U.S. surveillance to invalidate Safe Harbor, the E.U.-U.S. data transfer agreement. CNAS also urges the U.S. to “publicly reinforce the significance” of the surveillance constraints in Privacy Shield, Safe Harbor’s successor. The report singles out the U.S.
establishment of an ombudsperson in the State Department to address EU residents’ complaints. Here, my take is more clearly prescriptive than the CNAS report. The State Department ombudsperson position lacks a concrete written account of that official’s powers and access to intelligence information. The ombudsperson’s spare job description could lead cynics to believe that the position’s power rests solely on the good graces of the U.S. intelligence community. That lack of independence would vindicate the CJEU’s skewed perspective in Schrems, and jeopardize Privacy Shield’s ability to withstand judicial scrutiny. To reduce these risks, the U.S. should put more meat on the bones of the ombudsperson’s authority.

The lack of clear visibility on the incoming Administration’s plans makes the CNAS report even more compelling. President Trump will have an urgent need for straightforward counsel. Congress needs insight of the same caliber. Up to now, the best guide has been David Kris’s paper here. That excellent paper focuses on Section 702. CNAS’s lucid report is essential because it situates Section 702 reauthorization in the overall context of U.S. surveillance. In this sense, it provides a valuable blueprint for future dialog between Congress, the Executive, and the public.

Topics: Privacy Paradox, Surveillance, FISA: 702 Collection

Peter Margulies is a professor at Roger Williams University School of Law, where he teaches Immigration Law, National Security Law and Professional Responsibility. He is the author of Law’s Detour: Justice Displaced in the Bush Administration (New York: NYU Press, 2010).