Jean Monnet Center of Excellence

Georgia Tech Center for European and Transatlantic Studies

The Sam Nunn School of International Affairs

The USA Freedom Act: A Partial Response to European Concerns about NSA Surveillance

Peter Swire

Working paper GTJMCE-2015-1

This working paper along with others in the same series can be found online at:
http://inta.gatech.edu/jmce/working-papers

Sam Nunn School of International Affairs
Georgia Institute of Technology
Atlanta, GA, 30332

Co-funded by the Erasmus+ Programme of the European Union

The **Jean Monnet Centre of Excellence** engages with Europe's place in a changing world with an American reference point, but a broader focus. It considers the bilateral relationship (specifically the Transatlantic Trade and Investment Partnership (T-TIP) negotiations); triangular diplomacy towards Russia; transatlantic competition over global rules (particularly with respect to data privacy); and the EU's role in peacekeeping.

The Centre is designed to leverage existing expertise at Georgia Tech; to foster new inter-disciplinary collaboration; and to engage audiences within and beyond the campus. To that end it draws together an interdisciplinary team of scholars f rom across the Ivan Allen College, as well as from the Scheller College of Business. It is funded with support from the European Commission (Jean Monnet Center 2014-1842). The working papers reflect the views only of their authors, and the Commission cannot be held responsible for any use which may be made of the information presented.

The Jean Monnet Center is housed in the **Center for European and Transatlantic Studies** (CETS), which serves as the locus for the Georgia Tech campus and the metro Atlanta community for research, teaching, and public events and programs related to the study of Europe, the European Union and the EU-U.S. relationship. Specifically, CETS aims to:

- promote and disseminate policy-relevant research that pertains to Europe and the transatlantic relationship;
- strengthen and expand the Nunn School curriculum and course offerings on Europe and transatlantic relations and lead an annual study-abroad program in Europe;
- provide a focal point for the local European diplomatic corps and transatlantic business community; and
- enhance public awareness and understanding of the EU-U.S. relationship.

The **Sam Nunn School of International Affairs** draws on its unique setting at one of the world's leading technological universities and on the unparalleled integrity and insight of the distinguished senator for which it is named to deliver innovative programs and cutting-edge research that integrate technology and the study of international affairs. At a time of rapid change, the School is dedicated to delivering programs in education, research, and public outreach that provide a greater understanding of factors that shape the world in which we live and work. The School strives to connect learning and experience through its interdisciplinary degree programs, policy-relevant research with a strong theoretical foundation, and regular interaction with practitioners.

Founded in 1990, the School enrolls more than 400 students in its bachelor's of science, professional master's, and research-focused doctoral programs. Twenty-two full-time faculty members teach and conduct research on a broad array of topics with a particular focus on how technological innovations affect national security, economic competitiveness, and prospects for international cooperation and conflict.

The USA Freedom Act:

A Partial Response to European Concerns about NSA Surveillance

Peter Swire

Abstract

In June 2015, the Congress adopted and President Obama signed the USA Freedom Act, the biggest pro-privacy change to U.S. intelligence law in nearly 40 years. To a significant extent it reflects recommendations suggested by President Obama's Review Group on Intelligence and Communications Technology. It also follows on from a series of pro-privacy reforms adopted by the Administration. Collectively, these reforms go a considerable way towards addressing European concerns about U.S. surveillance practices, although there is still a considerable way to go. The USA Freedom Act, although focused on domestic surveillance, provides encouragement that U.S. surveillance policy will continue to be reformed in a pro-privacy direction.

At the beginning of June 2013, the first story based on Edward Snowden's leaks hit the press – the U.S. government had assembled meta-data about many millions of Americans' domestic phone calls under Section 215 of the USA PATRIOT Act. Almost exactly two years later, Congress finished approval of the USA Freedom Act, ending bulk collection under Section 215. As one of five members of President Obama's Review Group on Intelligence and Communications Technology, I applaud passage of the new law, which is the biggest pro-privacy change to U.S. intelligence law since the original enactment of the Foreign Intelligence Surveillance Act in 1978.

This article highlights the close fit between the Review Group's work and the new law, as well as the multiple significant reform measures the Administration has already adopted without legislative change. In this era of partisan gridlock, the U.S. system of government has proved more responsive and resilient than many skeptics had predicted. The article then turns to discussion of how the USA Freedom Act fits into a significant overall response to European concerns about NSA Surveillance.

The Review Group

Two months after the Snowden stories began, President Obama announced formation of the Review Group, tasked to find an approach "that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure." My own role on the Review Group was based on my work as Chief Counselor for Privacy under President Clinton, as well as ongoing writing on foreign intelligence, encryption, and related subjects. The four other members had diverse capabilities: Richard Clarke, cyber-security and anti-terrorism advisor to both President Clinton and George W. Bush; Michael Morrell, former Deputy Director of the CIA; Geoffrey Stone, noted civil libertarian and former Provost of the University of Chicago; and Cass Sunstein, noted legal academic and former Administrator of the Office of Information and Regulatory Affairs in U.S. Office of Management and Budget. I feel honored to have had the opportunity to work with four such distinguished experts.

The Review Group initially received a fair bit of public skepticism, such as statements that "the review panel has effectively been operating as an arm of the Office of the Director of National Intelligence" and "no one can look at this group and say it's completely independent." This skepticism was perhaps understandable, because four of the members had worked for Democratic Presidents and the fifth, Geoffrey Stone, had actually been the Dean who hired a young Barack Obama to the University of Chicago Law School faculty. Nonetheless, in actuality, the Review Group had freedom to pursue our mandate as we wished. We had expert staffing from the relevant agencies, and received full briefings on every issue we asked about. The actual drafting was done entirely by the five members, resulting in a unanimous report with 46 recommendations and 304 pages, which was subsequently reprinted by the Princeton University Press.

When the Report became public in December, 2013, the greatest public attention focused on this statement: "Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders." This finding of "not essential to preventing attacks" had credibility because it was based on top-secret briefings to a group that contained senior experts in intelligence and counter-terrorism. A common response to civil liberties concerns says: "If you knew what we knew, you would want this surveillance power." After the Review Group report, that response was much harder to make in defense of Section 215 bulk collection.

The Review Group and USA Freedom

We next turn to the close fit between Review Group recommendations and the provisions of the USA Freedom Act. In doing so, passage of any legislation such as USA Freedom has innumerable parents, each of whose support turns out to be vital to eventual enactment. For this law, vital support came from these among others: the President, the intelligence community, and the administration generally, which supported the law; the members of Congress who brought together a unique coalition in both the House and the Senate; the Privacy and Civil Liberties Oversight Board, whose detailed report on Section 215 raised numerous compelling concerns with the program; and coalitions of outside supporters from the political left and right, from industry and civil society.

With the roles of innumerable others in passage clear, here is what USA Freedom provides, linked to Review Group recommendations:

- Recommendation 1: issue a Section 215 order only with judicial approval and heightened standard. The administration had already adopted this approach, and USA Freedom confirms it legislatively.
- Recommendation 5: End government storage of bulk telephone data and have records held in the private sector, accessible only with a judicial order. USA Freedom does this.

- Recommendation 2: Place similar limits on bulk collection using National Security Letters. USA Freedom applies the limit on bulk collection to NSLs and to FISA pen-trap orders.
- Recommendation 4: Have a general rule limiting bulk collection, absent extraordinary circumstances. USA Freedom does not enact this sort of general rule. On the other hand, any agency lawyer going forward has received a loud and clear message from Congress to be cautious before saying there is legal authorization for a new bulk collection program.
- Recommendations 9 and 10: Create greater transparency in government reports and allow greater transparency in company reports about the nature and extent of foreign intelligence orders. USA Freedom takes important steps for both of these.
- Recommendation 28: Create public interest advocates to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court (FISC). USA Freedom creates a panel of experts to file amicus briefs in this way.

That list exhausts the main substantive provisions of the USA Freedom Act, suggesting that the Review Group report played a constructive role in crystallizing specific reforms that could eventually make it through the legislative process. As I have written elsewhere, the administration itself has made significant intelligence reforms, led by the President himself. I believe President Obama himself was in an unusually good position to weigh the competing equities about intelligence reform: he taught constitutional law at the University of Chicago, and so is deeply versed on the civil liberties issues; he has been Commander in Chief of the armed forces during a period of

active combat, so that he has a trained and personal sense of responsibility about protecting the nation and its allies; and, he ran as the "Internet" candidate, using new communications technologies in innovative ways. Civil liberties, national security, and high-tech – these are obviously key areas relevant to any review of intelligence and communications technology. I believe the President's leadership on these issues confirms the good-faith nature of current surveillance changes.

U.S. Reforms and EU Concerns

We next examine how this U.S. legislative change fits into European concerns about U.S. surveillance in the wake of the Snowden revelations. The European view of American surveillance matters at this time. The EU is deep into its process of crafting a comprehensive new Data Protection Regulation, which will harmonize the disparate national privacy laws, and also create new rules for how personal data can flow to the United States and other countries. The current Safe Harbor that governs EU-US data flows is also in play, and heavily criticized by privacy hawks in Europe. Privacy supporters in Europe have been greatly strengthened by the widespread distrust of US surveillance, especially in Germany after widespread press reports of US wiretapping of Chancellor Merkel. Also, after so many surprises about the extent of NSA action, any claim that the US is amending its intelligence practices is greeted with considerable skepticism.

On its own terms, the USA Freedom Act could be seen as an underwhelming response to the concerns of European and other US allies. The limits on bulk data collection, after all, most dramatically affect US domestic communications, and there are no new statutory limits on US surveillance overseas. Nonetheless, the magnitude of US surveillance reform in the past two years is much greater than many realize, and passage of the new law has indirect effects that should be encouraging to European privacy observers.

Transparency. The Obama administration has taken important measures already to improve transparency (and thus accountability) about surveillance practices. Concerning the Foreign Intelligence Surveillance Court, the administration has systematically and thoughtfully declassified a large volume of court decisions, while shielding identities of sources and other correctly-classified information. This new approach to FISC decisions addresses the previous and potentially severe problem of secret law. A 2014 agreement with the Justice Department addressed a top priority of US-based technology companies, enabling them to provide considerably more information in the transparency reports that they now issue about government requests for communications data. The USA Freedom Act continued this trend, adding more US government transparency provisions and statutorily affirming the companies' ability to be more transparent about their responses to lawful access requests.

Presidential Policy Directive 28. For EU citizens the most path-breaking changes come from a document whose importance deserves a catchier title than

"Presidential Policy Directive 28." Issued in January 2014, PPD 28, as a matter of principle, changes the ancient tradition that no-holds-barred spying on foreign countries should be expected, even when legal rules limit wiretapping and other surveillance on the home country's citizens. For the NSA, there have long been pervasive rules that limit the handling of information about "US Persons" – US citizens and permanent residents. For instance, minimization rules mean that analysts see information about "US Person 1" or "US Person 2" rather than the name, and dissemination rules limit when US Person information can go to other federal agencies.

In PPD 28, the baseline rule for intelligence becomes that non-US Persons will be treated with the same safeguards as US Persons, except where there is a reason to act otherwise. Under the new regime, actionable intelligence in a war zone would presumably be provided in full detail, but the daily activities of a German or French citizen would generally be treated under the same rules that apply to US persons in those countries. This approach addresses the European concern that their citizens are not being treated with respect, and dovetails with what European fundamental rights lawyers call a necessary and proportionate approach to surveillance. Indeed, no European or other country has announced any similar rules for its own intelligence agencies.

European leaders have expressed support for the new principles announced in PPD-28, but also skepticism. Why, after all the stories in the *Guardian* and elsewhere, should Europeans believe any US government statements about the scope of NSA surveillance? I believe the general public has good reason to believe such statements.

The Review Group found reassuringly strong compliance with law in those carrying out signals intelligence. In the aftermath of September 11, it is true that the legal basis of new surveillance programs was shaky at best and programs to assure compliance were lacking. The Review Group found, however, that that had changed over time: "The hard work and dedication to mission of NSA's work force is apparent. NSA has increased the staff in its compliance office and addressed many concerns expressed previously" by the Foreign Intelligence Surveillance Court. A National Research Council report, similarly based on access to highly classified material, agreed, finding "automated and strong manual controls in place" in the NSA, as well as "rigorous auditing and oversight processes."[1] Going forward, those sorts of auditing and oversight processes will exist for PPD-28.

Judicial redress for non-US persons. An issue that has long troubled European privacy experts is that the U.S. Privacy Act, which governs federal agencies and provides protections such as the right of individuals to access their own records, applies only to US Persons. The Review Group recommended amending the statute to include non-US Persons. Today, the Department of Homeland Security applies the Privacy Act the same to US and non-US Persons (except it cannot create a private right of action for the latter). The US Attorney General has announced that the administration supports legislative change to provide judicial redress (a private right of action) for non-US persons as well. Leaders in the House of Representatives are working on a bill, and major technology companies, mostly publicly Google, are supporting this reform.

[1] National Research Council, Committee on Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals intelligence Collection, at S-4.

Greater White House oversight of the Intelligence Community. Within the executive branch, the administration has announced a number of measures to inject a broader range of views into areas traditionally decided within the intelligence community. Sensitive international data collection, including targeting of foreign leaders, is now done through White House procedures that draw on the insight of economic and diplomatic policy leaders. A similar new White House process exists for what are called "zero day exploits." That process essentially weighs the equities about when to keep a software flaw secret to enable intelligence or military offensive actions versus when to inform the software companies about a vulnerability that needs to be fixed.

Funding for reforms. Some progress was made last year on funding needed reforms, with the possibility of additional change this year. Last year the independent Privacy and Civil Liberties Oversight Board, which has access to highly classified information about the intelligence community, received a large increase in funding. The administration supported a similar increase in funding for the Justice Department to handle requests under Mutual Legal Assistance Treaties, which are a desirable path for government access to individuals' communications overseas (as well as a focus of my own current research). The House provided that funding, but unfortunately the Senate did not. The administration is now pushing to get this funding in the current budget cycle.

USA Freedom as a sign of additional pro-privacy reforms. There are numerous signs, visible to European and other observers, that the United States is treating privacy more seriously as a policy issue. President Obama made prominent announcements on privacy and cybersecurity as part of his 2015 State of the Union Address. These included proposing legislative text for a Consumer Privacy Bill of Rights and supporting privacy protections in student records and elsewhere. This vocal support for privacy protections increases the hypocrisy costs of promising surveillance reforms while failing to implement them in practice.

The USA Freedom Act itself is the biggest single indication to date of the seriousness of current US concerns with privacy issues. Anyone who watches or reads the debates leading up to passage will see numerous members of Congress establishing a record for their strong support of privacy. Once sensitized to this issue in one context, it becomes more likely they will support privacy in other contexts. For example, Section 702 of the FISA Amendments Act has authorized the Prism program, where the content of emails and other communications, targeted at a non-US person outside of the US, is available to the NSA without a judicial order. Section 702 sunsets in 2017, and there have been loud calls for reforming that part of intelligence law before it is reauthorized.

Conclusion

In conclusion, even before passage of the USA Freedom Act, the US had made an under-appreciated variety of surveillance reforms, including measures to protect our

allies and their citizens. Further details on PPD-28 and other issues will emerge over time. We can appreciate these changes while continuing to push for needed reforms on Section 702, the Privacy Act, and in other areas. The Congress has just passed the biggest pro-privacy change to intelligence law in nearly 40 years, and allies of the US can take heart in the seriousness of the ongoing reform process.

About the author

Peter Swire is the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business, with appointments by courtesy in the School of Public Policy and the College of Computing. He is also Senior Counsel at Alston & Bird LLP. In 2013, he served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Prior to that, he was co-chair of the global Do Not Track process for the World Wide Web Consortium. He is a Senior Fellow with the Future of Privacy Forum and a Policy Fellow with the Center for Democracy and Technology. Under President Clinton, Swire was the Chief Counselor for Privacy, in the U.S. Office of Management and Budget. He is the only person to date to have U.S. government-wide responsibility for privacy policy. In that role, his activities included chairing a White House task force on how to update wiretap laws for the Internet age, and helping negotiate the U.S.-E.U. Safe Harbor agreement for trans-border data flows.