A protest against the United States' PRISM surveillance programs in Berlin, Germany. Photo by Mike Herbst, CC BY-SA 2.0, via Wikimedia Commons.

On International Privacy

A Path Forward for the US and Europe

BY MARC ROTENBERG

June 15, 2014

The United States and its closest allies may be on a collision course over the future of privacy in the networked world. Whether leaders are able to find a policy solution will require that they understand the significance of the recent NSA disclosure as well as the development of modern privacy law.

Long before a former NSA contractor spilled the secrets about the scope of the NSA's global surveillance, foreign governments worried about the ability of the United States to monitor those living in their countries. The increasing automation of personal information and the technological advantage that the United States enjoyed over other nations was already seen as a problem in the late 1960s. The concerns only increased as Internet-based commerce gave rise to the vast collection and storage of personal information by US-based companies.

But the Snowden revelations this past year have amplified the debate in a way that could not have been anticipated. The European concerns about the possible loss of privacy, in addition to US surveillance capabilities, have been made real by a flurry of PowerPoints that describe programs such as PRISM (a collection of Internet traffic in the US from US Internet firms under US legal authorities) and TAO (Tailored Access Operations — a variety of techniques used by the NSA to hack computer networks). The documents also reveal high levels of cooperation between US Internet firms and US intelligence agencies. Under the Foreign Intelligence Surveillance Act, the Internet activities of non-US persons — everything from emails to website visits and location data — are routinely transferred by Internet firms to US intelligence agencies.

The consequences of this disclosure for international policy are far reaching. Many countries are moving to update their privacy laws while seeking to limit the growth of US based cloud services that would store the personal data of non-US citizens, accessible to US intelligence agencies. Also, the already fragile structure of Internet governance is under increased scrutiny. Countries are skeptical of the US-based organization that manages the key functions of the Internet since it has shown itself unwilling to protect the privacy interests of Internet users. Additionally, the economic cost of the NSA programs are mounting for US businesses.

In this article, I trace the development of modern privacy law, recap the current state of mass surveillance, summarize several of the steps undertaken by President Obama to respond to the public concerns both in the US and Europe, and offer my own suggestions about what could happen next. In brief, the United States will need to do more to address concerns about NSA surveillance, particularly outside of the United States. First, the President must make good on the commitments to end the NSA bulk record collection program and adopt a majority of the recommendations of his expert panel. Second, he should move forward privacy legislation, based on his own proposal

for a Consumer Privacy Bill of Rights. Finally, the United States must support an international legal framework for privacy protection, such as the Council of Europe Privacy Convention.

Origins of Modern Privacy Law

To understand the significance of the current debate over NSA surveillance, it is necessary to return to the end of the Second World War and to the establishment of the United Nations. Many countries recognized the need to establish protections for basic human rights that would support democratic institutions. And so, as a modern right, privacy established a firm international foothold with the adoption of Article 12 of the Universal Declaration of Human Rights in 1948. This simple text established privacy's position as a fundamental human right and it was widely adopted in constitutions around the world. And not long after, as new European institutions began to emerge, the European Convention on Human Rights set out in Article 8 a robust concept of privacy, incorporating concepts of necessity, proportionality, and the functioning of a democratic state which have created a jurisprudence of privacy widely followed by European nations and influential countries around the world.

These two provisions — Article 12 of the UDHR and Article 8 of the European Convention — provided the cornerstones for the modern structure of privacy. They helped establish the sense that privacy, like freedom of expression, was a universal right which governments were obligated to respect.

As modern information systems emerged in the 1970s and 1980s, new frameworks were established with the Council of Europe Privacy Convention in 1981 and the Data Protection Directive of the European Union in 1995. Both the COE Convention and the EU Directive established legal rules for the transfer of personal data across national borders, notably with the goal of enabling the free flow of data while safeguarding fundamental human rights. Although the United States did not sign the

Council of Europe Convention or adopt the Data Protection Directive (it was eligible to ratify the former, but not the latter), the United States did support a comparable non-biding framework, the OECD Privacy Guidelines of 1980. These guidelines established a similar set of principles for transborder data flow. In short, these policy frameworks placed responsibilities on organizations that collect and use personal data while establishing rights for individuals, such as the right to inspect and correct data to ensure its accuracy and limited use. The aim was to promote transparency and accountability in data processing while enabling the development of new technologies and ensuring the protection of fundamental rights.

Through the early development of the Internet economy, questions increasingly arose about the adequacy of the US approach to privacy protection. Originally, the US argued for a "sectoral" approach to privacy protection, taking privacy on an industry-by-industry basis. But that argument gave way to proposals for self-certification and self-regulation, represented by such arrangements as the Safe Harbor. While Safe Harbor set out privacy guidelines for data flows between Europe and the United States, it lacked a meaningful enforcement mechanism. A related effort now underway at the Department of Commerce, which encourages "stakeholders" to develop "industry codes of conduct," reflects a similar view. Meanwhile, European institutions, moved to address new challenges brought about by rapid changes in technology, sought to update privacy rights by extending the reach of their data protection agencies.

The Impact of the Snowden Disclosures

For those who hoped to minimize the significance of Edward Snowden's revelations about US government-sponsored spying, the disclosures could not have come at a worse time. Europe was already in the midst of updating its general law for data protection and there was the widespread perception that the US government and US industry were actively opposed. The rapporteur for the Parliament committee responsible for moving forward the draft European legislation was besieged with

more than 4,000 amendments, each intended to slow or modify the proposed General Data Protection Regulation that would modernize European law. A website sprung up to track the influence of US corporations on the text of the legislation under consideration in the European Parliament.

Apart from the legislative debate over the future of the Regulation, other significant changes were occurring within European law and European institutions that favored stronger protections for privacy. The right of "information privacy," not just the privacy described in the Universal Declaration of Human Rights or the European Convention, had been recently incorporated within the Treaty of Lisbon, one of the foundational documents for the European Union. The document made information privacy a constitutional right for European citizens. Also, the allocation of authority among the European institutions, little more than two decades old, was continuing to evolve. More responsibility was granted to the European Parliament and the recently established European Data Protection Supervisor, a powerful advocate for the privacy rights of Europeans.

Moreover, the Europeans were reminded on almost a daily basis of the growing appetite of US Internet firms for data concerning European consumers. Data protection authorities in Spain were investigating the practices of US search companies. French officials were threatening an enforcement action against Google for violating French national data protection laws with a revised privacy policy that permitted the profiling of Internet users. In Ireland, an extensive investigation of Facebook had recently concluded, requiring the company to make extensive changes to its practices, not only in Europe but also in the United States. More than a dozen countries had opened investigations of Google Street View, the program which the company claimed was mapping city streets but was in fact also capturing wi-fi communications.

Thus, when the disclosure of mass surveillance by the NSA was revealed in the summer of 2013, it was hardly without legal, political or social significance. In fact, it

would be hard to imagine a time in the last fifty years when the disclosure of widespread surveillance by the US government in Europe could have elicited a stronger political response.

And so the European Parliament moved quickly. Less than a month after the first revelations were published, the Parliament adopted a resolution calling for a comprehensive investigation of the "Mass Surveillance of EU Citizens." Extensive hearings were held. Officials met with counterparts in the US. Subsequent reports that the NSA intercepted the private calls of foreign leaders only added to the firestorm. German Chancellor Merkel expressed strong public disapproval and Brazilian President Dilma Rousseff cancelled a long scheduled meeting with President Obama.

Europe was hardly alone in raising objections to the NSA programs. In the United States, opposition was widespread. A sweeping proposal to defund the NSA surveillance activities, introduced by a freshman Congressman Justin Amash (R-MI), gathered almost enough votes from House members, both Republicans and Democrats, to pass. The Electronic Privacy Information Center ("EPIC") filed a petition with the US Supreme Court, arguing that the program to collect in bulk the telephone records of US telephone customers exceeded the legal authority established in law.

The EPIC case gathered the support of dozens of legal scholars and former members of the Church Committee, who helped enact the original law intended to limit the surveillance authorities of the National Security Agency. (The Supreme Court dismissed the petition without ruling on the merits). Later in the fall, the well renowned Democratic chair of the Judiciary Committee, Senator Patrick Leahy, would join with the conservative leader, Congressman James Sensenbrenner, to sponsor the USA FREEDOM Act. The Act intended to roll back much of the NSA surveillance programs, and though Congress has yet to vote on the measure, more than 100 Members have signed on as co-sponsors.

The US Response

President Obama's initial response to the Snowden disclosures mirrored the statements of his intelligence advisors but they were not sufficient to address concerns in the United States and Europe. Obama appeared to think that if there was more openness and explanation for the program activities, public support would follow. But it became clear that substantive changes were needed to address opposition in the United States and the criticism of its allies.

At a news conference about a month after the initial disclosures, President Obama took the first steps toward reform. He said he would revise the controversial section 215 program that permitted the bulk collection of American telephone records. The President announced that he would "take steps to put in place greater oversight and greater transparency."

He also said that he favored the establishment of a public interest advocate to argue at the Foreign Intelligence Surveillance Court, a move favored by civil liberties advocates and former judges on the secretive court, but one that would not actually limit the scope of the surveillance program. The President further said that he would disclose more of the activities of the secretive Foreign Intelligence Surveillance Court, appoint a privacy officer for the agency, and create a website to make the agency programs more transparent.

Finally, the President announced the creation of a high level expert group, including former White House advisors, to make specific recommendations for changes in intelligence gathering activities. That expert group would eventually produce a report with far more sweeping recommendations.

The President's speech was intended to set out concrete steps for reform and to address criticisms about the scope of the NSA programs that were known at the time. But there was too little in the announcement to satisfy foreign governments and too much was still to be released by Snowden. Foreign governments were also becoming increasingly critical of the NSA's practices, and a move toward non-US based computing services was emerging.

The President then returned to the topic at a speech in January 2014. That speech had the benefit of the report from the President's expert group which recommended a dramatic overhaul of the NSA's activities. The review panel called for an end to the bulk collection of telephone data in the US that had triggered various lawsuits. It also recommended the narrowing of surveillance on foreign government and foreign leaders. The review panel said that the NSA had to stop subverting Internet security standards and called for the establishment of new oversight mechanisms.

The President did not endorse all of the recommendations, but he did make a commitment to implement a majority of the proposals. He also announced that the NSA's bulk collection of telephone records would end. He further set out a new Presidential Policy Directive on signals intelligence which intends to narrow the scope of US spying on foreign leaders and foreign nations.

But by this point far more was known about the scope of NSA surveillance and opposition to the Administration was increasing. Although the President had embraced significant reforms, the responses were mixed and European leaders in

particular continued to express concerns about the mass surveillance practices of the US government.

The Internet Governance Dimension

The current dispute over the scope of US surveillance also has implications for the future of Internet Governance. For many years, the United States defended an Internet management system that placed a US-based corporation,"ICANN" (the Internet Corporation for Assigned Names and Numbers), at its hub. The Internet Governance system was never stable, but until now, most serious threats to its future have been beaten back.

This may also change with the Snowden revelations and the news of the NSA's widespread surveillance. Nelie Kroes, the EU Commissioner for the Digital Agenda, said recently that countries now need to move from ICANN to a model that is "transparent, accountable and inclusive," views that echo earlier statements by EU Commissioner Vivian Reding.

It has become increasingly difficult for the United States to decouple the debate over the future of Internet governance from the reality of NSA surveillance. Too much of Internet policy is tied to decisions about security and stability which rest on technical standards that many fear the NSA has compromised. Internet advocates strongly favor a global, seamless network. But the movement toward regional Internets may come about for the practical reason that national governments and non-US firms may have no choice if the US-led Internet is unable to protect their interests. Recent comments by Chancellor Merkel make clear the concern as she is calling on France and other countries to lead an EU-based effort that would avoid reliance on US Internet firms

The increasing effort to develop cloud-based services outside of the United States reveals the potential scope of the problem. One estimate suggests that US firms could lose between US $30 billion and US $180 billion over the next five years if non-US firms conclude that data storage in the US, and the prospects of easy access by the NSA, no longer provide a viable business model.

What Happens Next

It is clear that the President will need to go further to address concerns about the scope of NSA surveillance, particularly outside of the United States. This raises a crucial question: What should happen next? I propose the following steps based on what the President has already endorsed, what the Europeans expect, and ultimately, what will need to happen to address long-term concerns about privacy in our data-driven age.

First, the President must make good on his commitments to end the NSA telephone record collection program and to adopt the recommendations of his expert panel. The fact that he has committed to these steps is no guarantee that they will occur.

To enact these changes, he will need the support of a Congress that has been notoriously unhelpful. He will also need the leaders in the intelligence community to understand that the strategy of simply giving the public more details about the NSA programs will not succeed. The NSA must be prepared to curtail the activities that gave rise to the protest. That means ending the collection of telephone records and Internet metadata on people who are not suspected of links to terrorist activity. This should be a blanket rule for both US and non-US persons.

The President must also move to implement the recommendations of his expert panel. Rarely has a government report set out as crisply and clearly the steps necessary to resolve a national controversy. While some proposals require support from Congress, many of the 46 recommendations can be put in place without Congress.

The President can move to strengthen oversight mechanisms and accountability through revisions to Executive Orders that he already controls.

He can also announce support for the USA FREEDOM Act, the primary legislative vehicle for implementing the recommendations of the review group. The President has been reluctant to engage in many legislative battles, but he will send a powerful message in this instance to the country and US allies if he makes clear that he favors legislative reform.

Second, the President needs to update privacy laws in the United States to more closely align US policy with European policy. In early 2012, President Obama set out a proposal for a Consumer Privacy Bill of Rights, which he described as a "blueprint for privacy protection in the digital age." It is an accurate assessment, reflecting many of the core principles present in the privacy frameworks described above.

It is also a framework widely supported by consumer organizations in the United States and Europe. The problem is that the President has done little to move the proposal forward. As a consequence, those outside of the United States wondering whether US Internet firms are going to protect the privacy of their non-US customers still remain skeptical. And in the United States, Internet users continue to confront unparalleled levels of identity theft, security breaches, and credit card fraud. President Obama could address these concerns by pushing forward with a modern framework for privacy protection in the United States, which he has already outlined.

Finally, the US will need to do more to support a viable international framework for privacy protection. It is a well known paradox that promoting the free flow of personal data across national boundaries requires comprehensive privacy protection. That is the foundation of trust for networked-based services. This insight led the European countries to establish a common framework for data protection within the European Union. But the Data Directive applies only indirectly to non-EU states.

For this reason, the United States should move to ratify the Council of Europe Convention on Privacy, the most widely known international framework for privacy protection. Some may object to the US supporting a Council of Europe convention, but it was only a few years ago that that the US rallied its European allies behind the COE Cyber Crime Convention, an international treaty which the US strongly supported.

The recent disclosures about the scope of NSA surveillance have not only made clear the need to reform the activities of the intelligence community, but they have also brought attention to the need for the United States to update its privacy laws and to put into place an international framework for privacy protection. The White House has already taken several significant steps in this direction. But there is more to be done. If the United States does not take bold steps now, not only privacy, but also global commerce and the future of the Internet, will be at risk.

Related Articles

Sino-Indian Relations: History, Problems and Prospects

BY KESHAVA GUHA

October 19, 2012

Henry Kissinger and Robert Mugabe: The Forgotten Connection via Remarkably

Creative Negotiation

BY JAMES K. SEBENIUS

February 28, 2018

Eyes on the Prize: Nobel Laureates in East Asia

BY EUNICE LEE

November 20, 2014

Why the EU Should Decouple Sanctions Against Russia from the Minsk Agreements

BY ANDREAS UMLAND

July 15, 2016