epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

March 11, 2019

The Honorable Lindsey Graham, Chairman
The Honorable Dianne Feinstein, Ranking Member
U.S. Senate Committee on the Judiciary
Dirksen Senate Office Building 224
Washington, DC 20510

Dear Chairman Graham, Ranking Member Feinstein, and Members of the Judiciary Committee:

We write to you regarding the hearing on "GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation." EPIC has published widely on the significance of the GDPR, the need for federal baseline legislation, and how privacy law promotes innovations. Please contact us if you would like more information.

We ask that this letter and the attachments be entered in the hearing record.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

Attachments

Marc Rotenberg, *America Needs a Privacy Law*, New York Times (December 25, 2018)

Marc Rotenberg, *Congress can follow the EU's lead and update US privacy laws,* Financial Times (June 1, 2018) ("Regarding innovation, it would be a critical mistake to assume that there a trade-off between invention and privacy protection. With more and more devices connected to the Internet, privacy and security have become paramount concerns. Properly understood, new privacy laws should spur the development of techniques that minimize the collection of personal data.")

Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation*, Techonomy (May 4, 2018)

Marc Rotenberg, *Promoting Inovation, Protecting Privacy,* OECD Observer (June 2016)

Marc Rotenberg, *On International Privacy: A Path Forward for the US and Europe,* Harvard International Review (June 1, 2014)

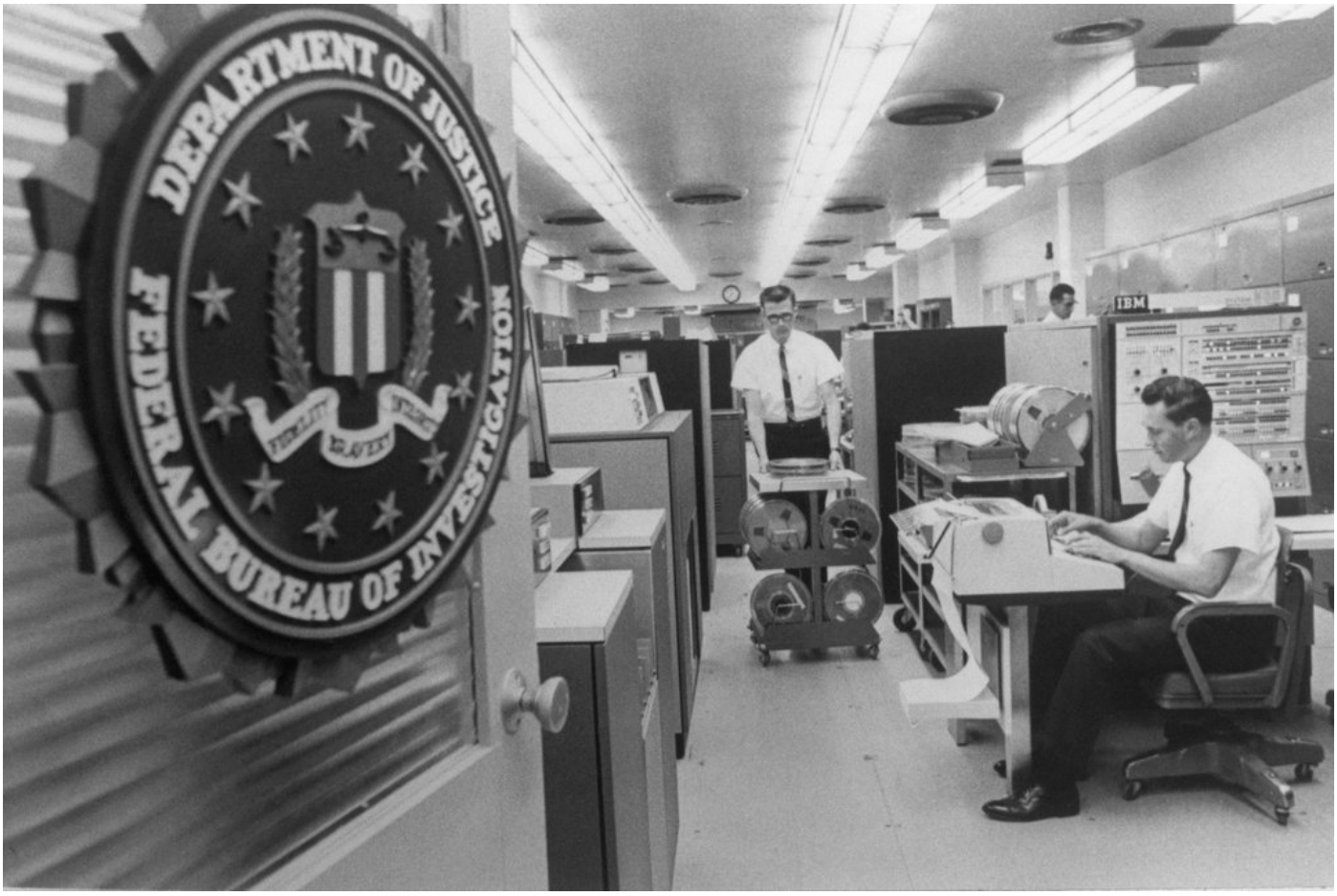
America Needs a Privacy Law

Dec. 25, 2018

letter

An expert on data privacy says the United States lags behind Europe.

A view of the F.B.I. National Crime Information Center in Washington in 1967. In the 1960s, lawmakers began to question the government's gathering of Americans' data.Bettmann, via Getty Images



A view of the F.B.I. National Crime Information Center in Washington in 1967. In the 1960s, lawmakers began to question the government's gathering of Americans' data.Bettmann, via Getty Images

To the Editor:

"The End of Privacy Began in the 1960s," by Margaret O'Mara (Op-Ed, Dec. 6), points to several critical moments in the development of American privacy laws, but there is much in this history that needs clarifying if the next steps on privacy are smart ones.

Ms. O'Mara is correct that the proposal for a National Data Center and growing concern about the misuse of personal data by the government culminated in the Privacy Act of 1974. But a deal with the Ford White House stripped the final bill of private-sector coverage and a dedicated federal agency. The country has lived with the consequences.

Coverage in the private sector is uneven or exists not at all. The absence of a privacy agency is still a gaping hole in American law. The Europeans, building on the United States' experience and facing similar challenges, managed to develop a privacy regime that is both more coherent and more effective.

Back then, Congress well understood the need to limit the collection of personal data. And Congress did not view privacy protection and the free flow of information as a trade-off. In the same year that Congress enacted the Privacy Act, it also strengthened the Freedom of Information Act.

There is still much that Congress can do to strengthen privacy protections for Americans. Enacting federal baseline legislation and establishing a data protection agency would be a good start.

Marc Rotenberg
Washington
The writer is president of the Electronic Privacy Information Center, teaches at Georgetown Law and frequently testifies before Congress on privacy issues.

Congress can follow the EU's lead and update US privacy laws

From Marc Rotenberg, Washington, DC, US

May 31, 2018

Contrary to the views of Wilbur Ross, US commerce secretary, many Americans welcome the new privacy law of the EU and look forward to its adoption by US companies (Opinion, May 31).

Today internet users face unprecedented levels of identity theft, financial fraud and data breaches. According to the Federal Trade Commission, identity theft is the second biggest concern of American consumers, just behind debt collection.

In 2015, a breach of the US Office of Personnel Management affected 22m federal employees, their friends and family members. The Equifax breach compromised the authenticating details of most adults in the US.

Congress has failed to update US privacy laws and US consumers pay an enormous cost each year. The current self-regulatory regime has left companies, many of whom want to be good on privacy, unclear about what they should do. That may explain why many US businesses have simply decided to support GDPR for all users.

And many of the GDPR's provisions can be found in privacy laws around the world, including the US. The US developed the first comprehensive approach to data protection and also backed an international framework to promote transborder data flows, adopted by the OECD. But the US has failed to extend privacy protection to internet-based services and we now live with

consequences.

Regarding innovation, it would be a critical mistake to assume that there is a trade-off between invention and data protection. With more and more devices connected to the internet, privacy and security have become paramount concerns. Properly understood, new privacy laws should spur the development of privacy enhancing techniques that minimise the collection of personal data.

Instead of criticising the EU effort, the commerce department should help develop a comprehensive strategy to update US data protection laws.

But it has also shown a deaf ear to privacy concerns with the recent decision to add a question about citizenship status to the census, a proposal that is widely opposed by US civil rights groups.

Marc Rotenberg
President, Electronic Privacy Information Center (EPIC), Washington, DC, US

The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation

Marc Rotenberg

(Image: Sjo/iStock Unreleased/Getty Images)

Not less than one month after Mark Zuckerberg told almost fifty members of Congress that he was sorry about the Cambridge Analytica debacle and promised to do better, Jan Koum, the co-founder of the popular messaging app WhatsApp, said he was leaving the Facebook board of directors. The reasons? Ongoing concerns about Facebook's business model and the protection of user data.

My organization — the Electronic Privacy information Center (EPIC) — is responsible for the 2011 Federal Trade Commission's consent order that was supposed to get Facebook to clean up its privacy practices after the Beacon fiasco. We were pleased that more than a dozen members of Congress raised the consent order with Zuckerberg during the hearings. Our key point to Congress was that the FTC's failure to enforce the consent order likely contributed to the Cambridge Analytica breach.

Even after the order, Facebook had little interest in what app developers did with the personal data of Facebook users. The company did not even bother to review Kogan's terms and conditions. The order that EPIC helped establish required comprehensive privacy program and routine audits by an independent third party. Did anyone at the FTC even bother to read the reports? Perhaps a future Congressional hearing will answer that question.

The Koum breakup with Facebook speaks to how the internet economy could evolve, how competition and innovation could be encouraged, if regulators simply do their job.

Koum's original model for WhatsApp was wildly popular. Robust security. Minimal data collection. Worldwide reach. No advertising. And all for 99 cents a year. By 2014, WhatsApp had 500 million users. Koum was also a hero in the privacy world. A Ukrainian with a strong aversion to surveillance, Koum wrote "no one wakes up excited to see more advertising; no one goes to sleep thinking about the ads they'll see tomorrow."

The backstory

There is a long, complicated story about Zuckerberg's courtship of WhatsApp, Facebook's largest acquisition to date, but the interesting regulatory story concerns what Facebook would do with the data of WhatsApp users once it acquired the company. Koum understood the problem. And so did we.

In March 2014, EPIC filed a complaint with the FTC concerning Facebook's proposed purchase of WhatsApp. As we explained at the time:

"WhatsApp built a user base based on its commitment not to collect user data for advertising revenue. Acting in reliance on WhatsApp representations, internet users provided detailed personal information to the company including private text to close friends. Facebook routinely makes use of user information for advertising purposes and has made clear that it intends to incorporate the data of WhatsApp users into the user profiling business model. The proposed acquisition will therefore violate WhatsApp users' understanding of their exposure to online advertising and constitutes an unfair and deceptive trade practice, subject to investigation by the Federal Trade Commission."

We explained to the Commission that Facebook incorporates user data from companies it acquires, and that WhatsApp users objected to the acquisition.

Koum responded less than two weeks later: "Above all else, I want to make sure you understand how deeply I value the principle of private communication. For me, this is very personal." He added, "Make no mistake: our future partnership with Facebook will not compromise the vision that brought us to this point."

Two weeks later, in April 2014, the director of the FTC Bureau of Consumer Protection wrote to us, "if the acquisition is completed and WhatsApp fails to honor these promises, both companies could be in violation of Section 5 of the FTC Act and potentially the FTC's order against Facebook." The FTC letter concludes "hundreds of millions of users have entrusted their personal information to WhatsApp. The FTC staff continue to monitor the companies' practices to ensure that Facebook and WhatsApp honor the promises they have made to those users."

So there it is. Once again. Assurance from the Federal Trade Commission to protect the privacy of internet users. Except they didn't.

A call for action

As the Facebook acquisition of WhatsApp moved forward, European antitrust regulators served Facebook with a questionnaire of more than 70 pages to determine whether the merger violated antitrust laws. But the FTC remained strangely silent.

Fast forward to August 2016, WhatsApp announced plans to disclose user information to Facebook, including phone numbers and other user data, that will be connected with Facebook profiles. Users would have 30 days to opt-out of data transfers to Facebook, we believed, in violation of the law and the FTC's order.

We reminded the FTC that it had warned the two companies they must honor their privacy promises to users. We wrote that WhatsApp's plan to transfer user data to Facebook for user profiling and targeted advertising — without first obtaining users' opt-in consent
contradicts numerous FTC statements and violates Section 5 of the FTC Act.

And the Federal Trade Commission responded a week later. The FTC stated that it prohibits companies from engaging in unfair and deceptive practices and will enforce its 2012 Consent Order with Facebook and will "carefully review" EPIC's complaint.

More than a dozen U.S. consumer organizations asked the Federal Trade Commission to pursue the complaint EPIC filed about WhatsApp's plan to transfer user data to Facebook.

But the FTC never acted.

Europe reacts

However, a different story unfolded outside the United States. In the fall of 2016, Germany's privacy regulator ordered Facebook to immediately stop collecting and storing user data from WhatsApp, and to delete all WhatsApp user data that has already been transferred. In a statement, German officials said that WhatsApp's new data transfer policy constitutes "an infringement of national data protection law." EU Commissioner for Competition Margrethe Vestager opened an investigation into WhatsApp's privacy changes, which contradicted previous commitments to users and regulators.

(The European Commission would eventually fine Facebook $122 million for "misleading" statements when the EU approved the WhatsApp takeover. The company claimed that it would not be possible to merge the two databases.)

And then India joined the international opposition to the WhatsApp privacy changes. India's Deli High Court ordered WhatsApp not to transfer to Facebook any user data that was collected prior to September 25, 2016, and to delete data of users who opted out of WhatsApp's new data transfer policy prior to that date.

Fast forward to April 2018: Jan Koum, the WhatsApp CEO, gave up his highly coveted seat on the Facebook board of directors. According to the Washington Post's Elizabeth Dwoskin, Koum and Facebook disagreed over the advertising model, mobile payments, and strong encryption.

And here is the lesson: If the FTC had stood behind its commitment to protect the data of WhatsApp users, there might still be an excellent messaging service, with end-to-end encryption, no advertising and minimal cost, widely loved by internet users around the world. But the FTC failed to act and one of the great internet innovations has essentially disappeared.

Still the story is not over. There is still the possibility that the Facebook-WhatsApp deal could be unwound. There are five new commissioners at the FTC. And Joe Simons, the agency's new chairman, recently told Congress that the U.S. government may have been "too permissive in dealing with mergers and acquisitions."

Marc Rotenberg is President of the Electronic Privacy Information Center. He will be speaking at Techonomy NYC on May 8-9, as part of our discussions on the impact of net giants. He also helped establish the .ORG domain, that enables and promotes the non-commercial use of the internet.

OECD Observer

Promoting innovation, protecting privacy

By Marc Rotenberg
June 2016

According to a recent poll, an overwhelming percentage of people believe that their information is not private. They want new rules about how companies and governments can use online data about them. Its global survey found that 83% believe new rules are required to compel governments and companies to handle data more responsibly, whether personal or medical data, or data picked up on social websites or other platforms where people routinely engage.

A recent report found the rate of data breaches accelerating and the cost to business and consumers increasing. Clearly action is needed.

But while governments have a critical role to play, they should be careful of the policy traps that have littered the privacy field in the past.

First, “balancing” is a popular term in the policy world. But balancing privacy protection with the availability of new services is the wrong starting point. Users want both innovation and privacy protection. They should not be asked to trade-off basic protections for new services. Governments and businesses should make a commitment to achieve innovation and robust safeguards for personal data.

Second, “notice and choice”–presenting boilerplate terms and conditions that users are expected to accept–is a bad choice for privacy policy. In the Internet economy, the markets for personal data are two-sided. Companies stand between the users and the advertisers. Internet firms collect personal data and then sell the user preferences to the advertisers. The user is not the customer, but the product. And the very large firms that dominate search and social networking provide little opportunity for users to switch service providers because they are no real alternatives. Traditional market mechanisms, built upon transparency and competition, simply do not exist for the end user seeking to protect privacy. That is why it is critical to establish baseline privacy standards as the foundation for the Internet economy.

Third “interoperability” is also a policy dead end online privacy. The global network brings together consumers and businesses from around the globe. The key to online privacy are common standards for data protection that simplify data exchanges and provide trust and confidence in new services. End-to-end encryption, data minimisation, and Privacy Enhancing Techniques–not “interoperability”–are obvious solutions to many of the privacy and security challenges facing users today.

Regrettably as user concerns about privacy have increased, and the risks of data breach and data theft have grown, many governments have followed these insufficient strategies, which have only increased public concerns.

The good news is that the OECD has been at the forefront of efforts to promote good policies and good technologies to promote growth and innovation while safeguarding privacy since the early days of the Internet. The OECD Privacy Guidelines of 1980 remain one of the most influential data protection frameworks in the world. The OECD Privacy Guidelines have provided the basis for national law and international agreements. For example, in the United States the OECD Privacy Guidelines provided the basis for the privacy law to protect the personal information of subscribers to cable television services. Of the many privacy laws in the United States, the subscriber privacy provisions in the US Cable Act are among the very best.

Now coupled with some of the recent innovations in privacy policy, including data minimisation and breach notification, the 1980 OECD Privacy Guidelines remain a good starting point for policymakers developing legal frameworks for privacy protection.

The OECD also promoted the use of robust encryption with the OECD Cryptography Guidelines in 1997. Encryption is a critical data security technique that has helped make the possible the growth of the commercial Internet. No doubt crypto will pose some challenges for government, such as concerns about access to data of targets of criminal investigations. But the costs of poor security measures are also very real. Data breaches continue to rise, leading to identity theft and financial fraud. Many companies are collecting data they simply cannot protect. Governments should actively promote strong encryption particularly for cloud-based services, because it is not possible for users and businesses to monitor the security standards of those who store data remotely.

Of course, hi-tech firms are not waiting for policy makers to solve these problems. Companies such as Apple and WhatsApp have decided to build in strong security techniques to protect the data that has been entrusted to them by their users. These companies should be supported for addressing privacy challenges.

Protecting the interests of citizens a key responsibility governments, Yet many governments have experienced data breaches, including medical records, tax records, and even voting records. The Internet drives innovation, productivity growth and communication. But it is also a harbinger of data breaches, identity theft, and financial fraud, all of which have trended up during the Internet era. Users are rightly concerned about the protection of their personal information. And the indicators all suggest the problems will accelerate over the next several years.

Governments have a central role to play, but they should avoid hollow solutions, slogans, and failed strategies. If they want the digital economy to grow strongly, there is serious work ahead.

For more on privacy,visit EPIC.org. For more on civil society and the digital economy, visit CSISAC.org

HIR HARVARD INTERNATIONAL REVIEW

On International Privacy

A Path Forward for the US and Europe

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.