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

April 29, 2019

The Honorable Roger Wicker, Chairman
The Honorable Maria Cantwell, Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Wicker and Ranking Member Cantwell:

We write to you regarding the hearing on "Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework."[1] EPIC has published widely on the need for federal baseline legislation, how privacy law promotes innovations, and the failure of the Federal Trade Commission to enforce the agency's own consent orders and consumer privacy.[2]

The Federal Trade Commission helps to safeguard consumers and to promote competition, but the FTC is not an effective data protection agency. Even when the FTC reaches a consent agreement with a privacy-violating company, the Commission rarely enforces the Consent Order terms.[3] Over a year has passed since the FTC reopened its investigation into Facebook following the unlawful transfer of 50 million Facebook user records to Cambridge Analytica.[4] The Commission has done nothing. EPIC, through a FOIA request, recently learned that the FTC has over 25,000 complaints about Facebook pending with the Commission.[5] Yet in the eight years since the FTC announced a Consent Order with Facebook, the FTC has not taken a *single* enforcement order against the company.

The 2011 Facebook Order was the result of an extensive complaint filed by EPIC and a coalition of consumer organizations in 2009, following Facebook's repeated changes to its privacy settings that overrode user preferences and allowed third parties to access private information without users' consent.[6] The FTC has an obligation to the American public to ensure that companies comply with existing Consent Orders. It is unconscionable that the FTC allowed this unprecedented

[1] *Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework*, 116th Cong. (2019), S. Comm. on Commerce, Sci., and Trans. (May 1, 2019), https://www.commerce.senate.gov/public/index.cfm/2019/5/consumer-perspectives-policy-principles-for-a-federal-data-privacy-framework.
[2] See attached.
[3] *See EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).
[4] *See* EPIC, #EnforceTheOrder, @FTC, https://epic.org/enforce-the-order/.
[5] EPIC, EPIC FOIA - FTC Confirms More than 25,000 Facebook Complaints are Pending (Mar. 27, 2019), https://epic.org/2019/03/epic-foia---ftc-confirms-more-.html.
[6] EPIC, et al, In the Matter of Facebook, Inc. (Complaint, Request for Investigation, Injunction, and Other Relief) (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

disclosure of Americans' personal data to occur. The FTC's failure to act imperils not only privacy but democracy as well.

Given the enormity of the challenge, the United States would be best served to do what other countries have done and create a dedicated data protection agency. An independent agency could more effectively utilize its resources to police the current widespread exploitation of consumers' personal information and would be staffed with personnel who possess the requisite expertise to regulate the field of data security.[7]

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

Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States* (2019)

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

Marc Rotenberg, *After Latest Facebook Fiasco, Focus Falls on Federal Commission*, Techonomy (December 21, 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, *Promoting Innovation, 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)

[7] *See* Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States* (2019), https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf.

THE TIME IS NOW: A FRAMEWORK FOR COMPREHENSIVE PRIVACY PROTECTION AND DIGITAL RIGHTS IN THE UNITED STATES

The United States confronts a crisis. Digital giants invade our private lives, spy on our families, and gather our most intimate facts for profit. Bad actors, foreign and domestic, target the personal data gathered by U.S. firms, including our bank details, email messages, and Social Security Numbers.

Our privacy laws are decades out of date. We urgently need a new approach to privacy protection. We must update federal laws and create a data protection agency specifically tasked with safeguarding the privacy of Americans. The time is now.

1. ENACT BASELINE FEDERAL LEGISLATION

We call for federal baseline legislation that ensures a basic level of protection for all individuals in the United States. We oppose the preemption of stronger state laws. U.S. privacy laws typically establish a floor and not a ceiling so that states can afford protections they deem appropriate for their citizens and be "laboratories of democracy," innovating protections to keep up with rapidly changing technology.

2. ENFORCE FAIR INFORMATION PRACTICES (FIPS)

Baseline federal legislation should be built on a familiar privacy framework, such as the original U.S. Code of Fair Information Practices and the widely followed OECD Privacy Guidelines. These frameworks create obligations for companies that collect personal data and rights for individuals. Core principles include:

- Transparency about business practices
- Data collection and use limitations
- Data minimization and deletion
- Purpose specification
- Access and correction rights
- Accountability
- Data accuracy
- Confidentiality/security

"Personal data" should be broadly defined to include information that identifies, or could identify, a particular person, including aggregate and de-identified data.

Federal law should also:

- Establish limits on the collection, use and disclosure of personal data,
- Establish enhanced limits on the collection, use and disclosure of data of children and teens,
- Regulate consumer scoring and other business practices that diminish people's life chances, and
- Prohibit or prevent manipulative marketing practices.

3. ESTABLISH A DATA PROTECTION AGENCY

Many democratic nations have a dedicated data protection agency with independent authority and enforcement capabilities. While the Federal Trade Commission (FTC) helps to safeguard consumers and promote competition, it is not a data protection agency. The FTC lacks rulemaking authority. The agency has failed to enforce the orders it has established. The US needs a federal agency focused on privacy protection, compliance with data protection obligations, and emerging privacy challenges. The agency should also examine the social, ethical, and economic impacts of high-risk data processing and oversee impact-assessment obligations. Federal law must establish a data protection agency with resources, rulemaking authority and effective enforcement powers.

4. ENSURE ROBUST ENFORCEMENT

Robust enforcement is critical for effective privacy protection. Arbitration clauses do not protect consumers and permit dangerous business practices to continue. If a company violates federal privacy law, consumers must be able to pursue a private right of action that provides meaningful redress without a showing of additional harm. Statutory damages are an essential element of an effective privacy law. Robust enforcement also requires independent action by State Attorneys General.

5. ESTABLISH ALGORITHMIC GOVERNANCE TO ADVANCE FAIR AND JUST DATA PRACTICES

The use of secret algorithms based on individual data permeates our lives. Concerns about the fairness of automated decision-making are mounting as artificial intelligence is used to determine eligibility for jobs, housing, credit, insurance, and other life necessities. Bias and discrimination are often embedded in these systems yet there is no accountability for their impact. All individuals should have the right to know the basis of an automated decision that concerns them. And there must be independent accountability for automated decisions. Protecting algorithms as a trade secret overprotects intellectual property and creates a barrier to due process. Trade agreements should uphold algorithmic transparency. Algorithmic transparency is central to algorithmic accountability.

6. PROHIBIT "TAKE IT OR LEAVE IT" TERMS

Individuals cannot have meaningful control of their personal data if the terms of service require them to waive their privacy rights. Furthermore, requiring individuals to pay more or receive lower quality goods or services if they do not waive their privacy rights is unfair and discriminates against those with less means. Federal law should require that consent, where appropriate, is meaningful, informed, and revocable, and should prohibit "pay-for-privacy provisions" or "take-it-or leave it" terms of service.

7. PROMOTE PRIVACY INNOVATION

Federal law should require innovative approaches to privacy and security, including strong encryption, robust techniques for deidentification and anonymization, and privacy enhancing techniques that minimize or eliminate the collection and disclosure of personal data, and make privacy by design an affirmative obligation. The consolidation of personal data with a small group of firms has stifled innovation and competition. Antitrust enforcement agencies should consider privacy interests in merger review. Mergers that fail to protect the privacy of consumers should be rejected.

8. LIMIT GOVERNMENT ACCESS TO PERSONAL DATA

Personal data held by companies are often sought by government agencies for law enforcement purposes. We do not object to the disclosure of specific records that are required for legitimate criminal investigations and obtained through an appropriate judicial procedure. However, there should be a clear standard in a privacy law for such disclosure. U.S. companies cannot disclose user data in bulk to government agencies.

Signed,
Americans for Financial Reform
Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Digital Democracy
Center for Media Justice
Color of Change
Consumer Action
Consumer Federation of America
Defending Rights & Dissent
Electronic Privacy Information Center
Media Alliance
Parent Coalition for Student Privacy
Privacy Rights Clearinghouse
Privacy Times
Public Citizen
Stop Online Violence Against Women
U.S. PIRG

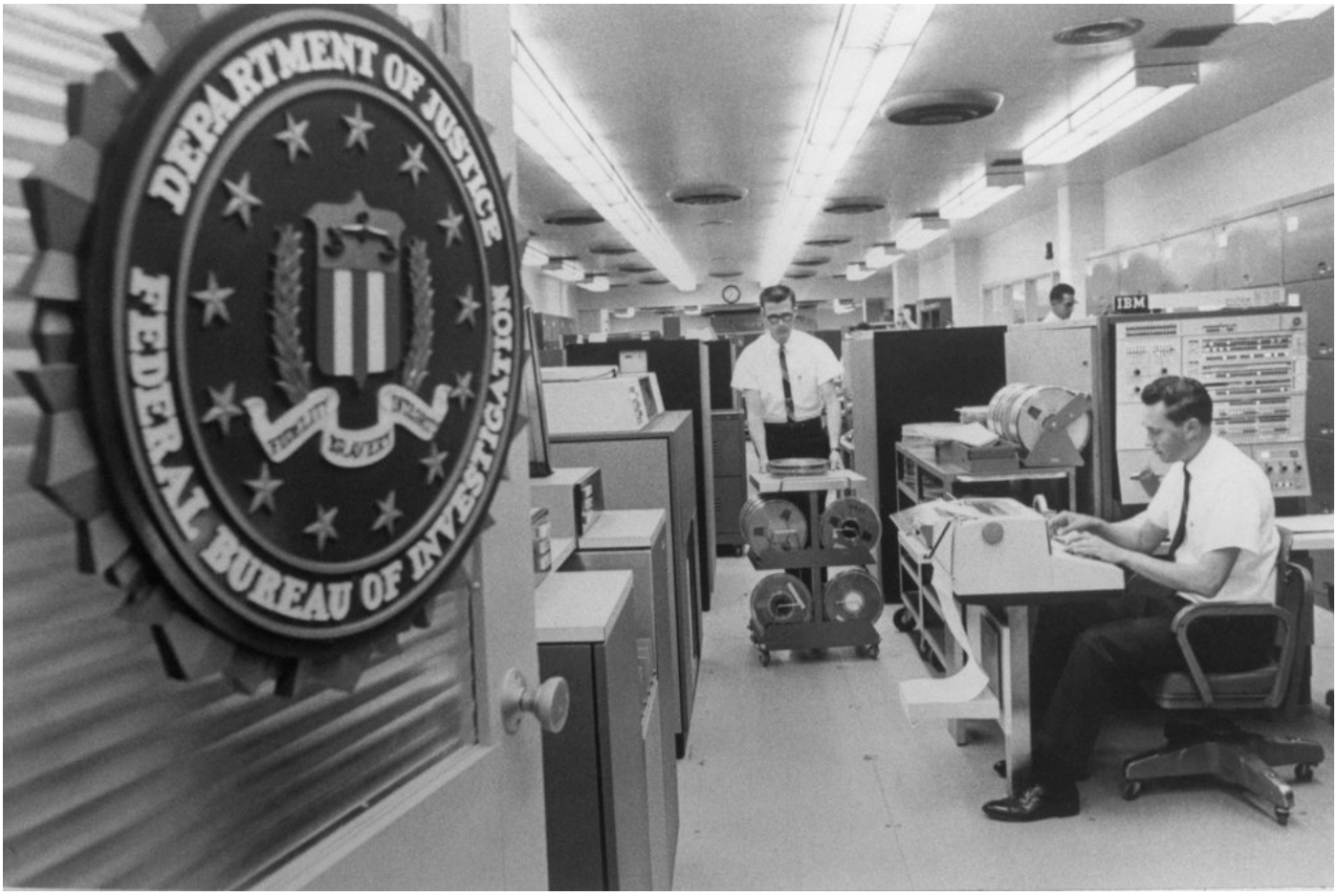
America Needs a Privacy Law

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.

After Latest Facebook Fiasco, Focus Falls on Federal Commission

Marc Rotenberg

Illustration for Techonomy by Mike McQuade

This week a *New York Times* investigation revealed that Facebook had secret deals with numerous companies for access to user data, including in some cases the contents of millions of users' private messages. The companies included Amazon, Sony, Microsoft, Yahoo, Spotify, and Netflix, as well as two firms considered security threats to the U.S.: Chinese smartphone manufacturer Huawei and Russian search engine Yandex.

This was hardly the first story about a massive Facebook privacy violation. In fact, many in the privacy world – and indeed anyone who pays close attention to policy challenges – may now be experiencing "Facebook fatigue." But it is hard to escape the sense that we have reached the tipping point – apologies will no longer work, education campaigns have reached a dead end, even informal agreements with members of Congress to reform business practices will not do the trick. So what happens next?

Much of the discussion is understandably on leadership at Facebook. Should Mark Zuckerberg and Sheryl Sandberg continue in their present roles? That

is a question being asked by shareholders, business journalists, and experts in leadership. But in the policy world, the focus is on the government agencies that are responsible for overseeing business practices and for imposing fines when companies cross the line.

And so the focus shifts to the new chair of the Federal Trade Commission, Joseph Simons. Simons joined the FTC in May, following his nomination last fall by Donald Trump. Simons came there after serving as a partner at a New York law firm that represents business groups facing antitrust charges. He had earlier served in the FTC's Competition Bureau in the first years of the George W. Bush administration.

At his nomination hearing before the Senate, Simons signaled he would take on the tech firms. He told the Senators that the FTC would prioritize the consumer protection issues "where harm is the greatest," and that would garner the "biggest bang for taxpayer dollar." (Note to reader: Facebook has 2.3 billion users.) Simons said "companies that are already big and influential can sometimes use inappropriate means, anticompetitive means, to get big or to stay big. And if that's the case then we should be vigorously enforcing the antitrust laws."

In July he told Congress, that the FTC needs greater authority to protect consumers. Simons asserted that privacy and data security are now the top priority for the FTC, and signaled his support for data protection legislation that would accomplish three things: (1) provide civil penalties for companies that violated the law; (2) give the FTC jurisdiction over nonprofits and common carriers; and (3) provide the FTC with rulemaking authority for privacy and data security.

Key to Simons present ability to act against Facebook is the sweeping 2011 consent order, that brought the company within the agency's legal authority

for 20 years. That legal judgement was supposed to end the practice of disclosing user data to third parties without meaningful consent, and required a comprehensive company privacy program and biennial third-party audits.

After 2011, the agency remained strangely silent about Facebook's post-consent order privacy violations, and even allowed it to acquire the data of WhatsApp users in an ill-considered merger in 2014. But in March of this year, the FTC announced it would reopen the investigation of Facebook, following news that the political data firm Cambridge Analytica, tied to President Donald Trump's campaign, obtained information on up to 87 million users of the social media site without their consent.

What might the Federal Trade Commission do now? That is a good question. Large monetary judgements may give some satisfaction but it is not clear how that would benefit users or advance the cause of privacy. And when the company's stock took a hit earlier this year, it responded by targeting its WhatsApp users with more advertising, a violation of commitments that both companies made to consumers prior to the deal.

Tim Wu makes a compelling case in his new book, *The Curse of Bigness: Antitrust in the New Gilded Age*, that now is the time to break up Facebook. The obvious candidates for separation are Instagram and WhatsApp. Those two companies provided competing services and could now in theory be available to Internet users who no longer want to give their personal data to the social media giant. In an earlier piece for Techonomy, I also explained that regulators could learn a lot from a closer look at the Facebook-WhatsApp deal. That merger was not only dreadful for privacy, but also for competition and innovation. And please reread that last sentence. The conventional wisdom that privacy and innovation are opposed is completely wrong.

But the clock is also ticking. It was in March that the FTC said "Companies who have settled previous FTC actions must also comply with FTC order provisions imposing privacy and data security requirements. Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook." The FTC thus confirmed, now almost nine months ago, that there was an open investigation into reported concerns about Facebook's privacy practices.

Since that time the British Data Protection Agency, facing similar concerns about the misuse of Facebook data during the Brexit campaign, conducted an extensive investigation, published a comprehensive report, and issued a substantial fine. And Elizabeth Denham, the UK Information Commissioner, has now produced a second report for Parliament that looks at data analytics and political campaigns, an issue that also needs greater scrutiny in the United States.

Joe Simons did not write the original consent order with Facebook, nor can he be held accountable for a half decade of inaction by the Commission. But he is now chair of the most powerful consumer agency in the country. He has the authority, the evidence, and the public support to act.

Marc Rotenberg is President of the Electronic Privacy Information Center, an independent research center in Washington DC, established in 1994 to focus public attention on emerging privacy issues. EPIC brought the original complaint to the FTC that resulted in the 2011 consent order with Facebook.

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

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.