Internet Policy Research Initiative
Massachusetts Institute of Technology

U.S. Privacy Legislation: Now Is The Time

Daniel J. Weitzner
Founding Director, MIT Internet Policy Research Initiative
weitzner@mit.edu

Boston Bar Association - Keynote address
2nd Annual Privacy & Cybersecurity Conference

21 May 2018

Daniel J. Weitzner
Founding Director, MIT Internet Policy Research Initiative
MIT Internet Policy Research Initiative[1]

I. Introduction

A string of privacy assaults -- beginning with the Equifax data breach and culminating in the large-scale misuse of personal data by Cambridge Analytica, enabled by Facebook -- raise the question: Is it time for the United States to enact a comprehensive privacy protection law? Some say, oh, the US already has 15 major federal privacy laws, covering everything from banking and consumer credit to health data and video rental records. These laws, plus a growing number of state laws and a robust tort system are plenty to protect American privacy values. Any more, goes the thinking just risks regulatory overkill and burdens on innovation. At the other extreme, some consumer advocates say: the US should follow Europe's lead and adopt a single, omnibus privacy protection law in the mode of the EU General Data Protection Regulation (GDPR).

I hope to convince you that the right path for the United States -- both for businesses and for citizens -- is somewhere in between. There are real gaps in the US privacy framework, leaving citizens with an abiding sense of distrust in the digital environment, which today means distrust in life in general. So claims from the past that there are no real privacy harms hold no weight in light of recent events. For businesses, the lack of clear privacy rules means both increasing uncertainty in the United States and the prospect, especially for information-intensive businesses, that their primary privacy regulator will be 4000 miles away in a different political jurisdiction. The US and Europe share many values in general, and have more in common on privacy than what separates us, but that does not mean that we ought to cede privacy jurisdiction to Europe altogether.

Efforts to pass comprehensive privacy law in the US began in the 1970s with the Federal Privacy Act of 1974. This was originally meant to cover all uses of personal data, both by the federal government and the private sector, but was scaled back to only cover the Federal government. Still, over the last forty years, the US has enacted a number of sector specific privacy laws, including protection for email and web browsing transactional records[2], protection of drivers license data,[3] children's online privacy,[4], health information privacy,[5] expanded protections for

[1] My sincere thanks to Peter Lefkowitz and Sayoko Blodgett-Ford, co-chairs of the conference, and to the Boston Bar Association for organizing such a timely conference.
[2] Amendments to the Electronic Communications Privacy Act, codified at 18 USC 2701, 2703(d) (1994).
[3] Drivers Privacy Protection Act, codified at 18 U.S.C. §§ 2721–2725 (1994)

financial records,[6], credit data privacy,[7] genetic information privacy.[8] In the early days of the Internet ecommerce era, Senator McCain together with Senators Kerry, Abraham and Boxer introduced the Consumer Internet Privacy Enhancement Act to much fanfare. There was debate but no bill passed. McCain and Kerry tried again in 2011 with the Commercial Privacy Bill of Rights. That also went nowhere. And then in 2012, President Obama proposed the Consumer Privacy Bill of Rights, with legislative language presented to Congress in 2015. That also failed to gain traction.

So Americans are certainly interested in privacy protection, but we just can't seem to decide what to do about it. There are, of course, the usual political barriers to passing privacy laws. Powerful industries such as advertisers and marketers, recently joined by their online competitors Google, Facebook and new online ad networks, all resist legislative intrusion on their ability to profile and target individual consumers. That may be changing as we see business leaders including Tim Cook from Apple, Marc Benioff from SalesForce and Brad Smith from Microsoft all calling for stronger privacy protection at the federal level. But I want to suggest that part of the reason we have trouble agreeing on what privacy law to pass is that privacy is complex and setting privacy rules entail resolving a number of real tensions between conflicting fundamental values.

II. Values

We talk about privacy in one word, as if it is one, clearly-defined concept. In actuality it is a bundle of values, all of which relate but some of which point in different directions. Consider the two major threads of privacy values in US law. First, the much beloved 'right to be let alone,' championed by Justice Louis Brandeis. He called this right "the most comprehensive of rights and the right most valued by civilized men[sic]."[9] Indeed, Brandeis and Warren's groundbreaking law review article[10] on the right to privacy was motivated by a personal concern that snooping newspaper photographers were trying to snap pictures for the society pages of Warren's daughters at private parties held in his fenced-off garden. Reaching back to 16th century English common law, our legal system has always held that 'a man's home is his castle,' impervious to intrusion by others. Yes, the Fourth Amendment only restrains government intrusion, but it also informs our culture and legal system more broadly about what the boundaries of privacy are. For example, in a challenge to FTC telemarketing rules

[4] Children's Online Privacy Protection Act, codified at 15 U.S.C. §§ 6501–6506 (1998)
[5] Health Insurance Portability and Accountability Act, Pub.L. 104–191. (1996)
[6] Financial Services Modernization Act of 1999, Pub.L. 106–102.
[7] Fair and Accurate Credit Transactions Act of 2003, Pub.L. 108–159.
[8] Genetic Information Nondiscrimination Act of 2008, Pub.L. 110–233
[9] Olmstead v. United States, 277 U.S. 479 (1928)
[10] Right to Privacy" 4 Harvard L.R. 193 (Dec. 15, 1890)

establishing the Do Not Call registry,[11] marketers argued that rules allowing individuals to avoid these calls violated the marketers' First Amendment Freedom of Speech rights under the United States Constitution. The court concluded to the contrary, that the US government has an important governmental interest in protecting individual citizens' privacy in their homes, citing the central role that privacy in the home as expressed in Fourth Amendment jurisprudence.

Yet privacy is not only about being left alone. An equally important privacy value in America law is the right to freedom of association enshrined in the First Amendment and most eloquently espoused in the landmark civil rights era case, NAACP v Patterson, challenging an Alabama state law that would have forced the NAACP and other civil rights organizations to disclose their membership lists to the state.[12] Justice Harlan wrote:

> "This Court has recognized the vital relationship between freedom to associate and privacy in one's associations.... Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."

Here, the Constitution protects privacy in order to preserve the very collective exercise of participation in our democracy through protest and dissent. So while the Fourth Amendment strand of our privacy tradition is ultimately about protecting the individual, the First Amendment strand is the quintessential example of the *collective* aspect of the right to privacy. And this same concern about avoiding potential chilling effects extends beyond just politics to religious, personal and even commercial interactions. A key part of why we protect privacy is to encourage people to feel free to express themselves in public without fear of retribution.

So even once we decide, as a society, that we want to protect privacy, there are a variety of values that must be satisfied in order to come up with the right legislative framework.

III. Harms that are not being addressed because of gaps in law

Today, citizens are suffering real privacy harms that are not effectively deterred by existing law.

A. Political Life - FB/Cambridge Analytica

Recent revelations about misuse of personal data by Cambridge Analytica show that there are harms from misuse of personal data to the political life of our nation. In this case, a Cambridge University research psychologist collected data from about 270,000 Facebook users through a

[11] Mainstream Marketing Services., Inc. v. FTC, 358 F.3d 1228, 1232-33 (10th Cir. 2004)
[12] NAACP v. Patterson - 357 U.S. 449 (1958)

personality profiling app installed by consenting users. As a result of Facebook's very permissive data access policies at the time, the researcher was able to collect data not only about those 270,000 but also their friends, who together, amounted to 87 Million users. Two intrusions actually happened here. First, the 87 Million users (not counting those 270,000 who actually installed the app) never agreed to have their data collected associated with a psychological profile of their friends. Second, and just as importantly, those 270,000 users were subject to a forced change in the context of their privacy relationship with both Facebook and Cambridge Analytica. They thought the data was going to be used in an a non-profit research context, but discovered that it was switched, without notice or consent, to a for-profit political context.

But what's the real harm?

Some privacy intrusions involving profiling used to target advertising or tailor services seem pretty innocuous. Though it may feel 'creepy' that some advertiser has inferred that you like red corduroys and plasters your mobile device with such ads, or that once you search for a home humidifiers on your computer, ads for the same product keep showing up on all the websites you visit across *all* of your devices. But is this anything more than a nuisance?

Cambridge Analytica's out-of-context misuse of person data went far beyond the norms of advertising and actually distorted our democratic process. Tens of millions of users who never agreed to be part of a survey ended up as the raw material used to develop the targeting models sold by Cambridge Analytica to various political groups who sought to manipulate the political discourse on Facebook. While the individual harm to each of those 87 Million users may have been small, the harm to our collective interest in democracy was substantial. Even though this *collective* privacy harm was real, we have no law on the books today to stop it from happening in the future.

B. Privacy in public life - smart cities

An emerging class of privacy harms is now being developed in our cities -- through so-called Smart City technology[13]. Cities are being highly instrumented today with large sensor networks set up to improve the efficiency of transportation services, help drivers find parking spaces more easily, and enable police do their jobs better by detecting potential criminal activity early. Today, the City of San Francisco tracks 25,000 bikes each day, a total of over 9 Million trips per year. Los Angeles uses Automated License Plate Readers to collect data on over 350,000 cars each day on Interstate 405 alone. In New York City, the LinkNYC free public wifi hotspots being

[13] Thanks to my students Wajeeha Ahmad (MIT IPRI), Elizabeth Dethy (MIT IPRI), Mandy Hix (Georgetown Law) and Boris Lubarsky (Georgetown Law) for their valuable research on smart city technologies.

placed all around the city collect technical data on each user device that connects to the Internet and has a forward-facing camera that collect images of bypassers. The Baltimore Police Department receives video footage from cameras placed around the city that allow it track the movements of citizens around the city. And gun shot spotting devices in San Diego can both detect gunshot sounds as well as ordinary conversations. Retail stores in cities are also getting into the act, with floor sensors and beacons that interact with shoppers' mobile devices to collect personal data and track shopping activity. Taken together, our cities now have an increasingly complete picture of citizens' daily activities.

In each of these cases, there is a legitimate, in-context use for the person data collected. At the same time, all of this sensor data, when analyzed over time and in combination with other information, can reveal highly sensitive information about people's daily habits, religious affiliations, personal relationships and many other very personal details. That is because the individual pieces of data collected add up to patterns that new machine learning algorithms and other analytic systems can use to infer these and other sensitive categorizations about individual lives.

No laws are in place to protect people from out-of-context use of that personal data. So we are putting citizens in a position of having to worry about whether going out in public will risk exposing sensitive details about their lives. The privacy harm here is not in the one-time collection of use of data, but more in the long-term storage and analysis of this data, and use later for purposes beyond the context in which it was collected. No one can properly make a privacy complaint about a speeding camera with automatic license plate reader catching them driving over the speed limit. But the data about all drivers, whether speeding or not, is collected and kept for the purpose of developing profiles of all of those drivers, then the data is being used out of context and is likely to harm each of us by chilling our behavior in public.

C. Privacy at Home - The Internet of Things

Just as our life is public in subject to new privacy intrusions, so too our home life. 'Always-on' devices such as the Amazon Echo, the Google Home and the Apple HomePod, are all competing to be our trusted helpers in our homes. They will play music, order pizza, or send flowers to a friend all on voice command. Through their ever-attentive ears, we can add to our shopping lists without touching a keyboard, check that the burglar alarm is on, or find out the weather outside. These devices also have long memories and increasingly sophisticated analytic capacity. So they will keep track of which household members are in the room and who is speaking. They can make inferences about mood from nuances of recorded speech. Other sensors built into these always-on devices can determine users heart rate, mood changes and even when there is sexual activity going on within earshot.

As with the public space sensors, there are productive and respectful uses of all of these technologies. At the same time, out-of-context misuse can spell real privacy risk. Of course, each household has a choice whether or not to install always-on devices. It is still too early to tell whether these services will become as ubiquitous as other Internet-era staples such as social networks and mobile phones. It is safe to say, however, that the core features of these devices offer such convenience that they will find their way into the privacy of many of our homes. So they will pose the same dilemma as other privacy-intrusive services.

IV. What do to?

Let's put this picture together: in our homes, in our online social interactions, in politics, and in public space, we *all* now face real risk to privacy. We are far, far from a world in which the law protects our 'right to be let alone.' We are also in a world where there are real threats to the values behind our First Amendment freedom of association. Where those threats come from government, we can look to the courts to protect us, but where they are from the private sector, the Constitution is merely a guide to legislators to help strengthen legal privacy protections. While we have strong privacy laws in many sectors, there are real gaps that must be filled.

So what would it mean to fill the gaps that the Internet has left in the US privacy fabric?

A. Example: Just add 'respect for context' to FTC Act as predicate for 'unfair' practice.

From 2010-2012, I led an effort in the Obama Administration to evaluate the state of privacy protection in the United States in light in increasingly connected digital life and the importance of Internet and information industries in the United States. The result was then-President Obama's proposed Consumer Privacy Bill of Rights of 2012[14]. I'll highlight two substantive provisions designed to address the challenges of privacy in this increasingly interconnected age.

First, it provided a right of individual control: "Consumers have a right to exercise control over what personal data companies collect from them and how they use it." This right is necessary but not sufficient. The Cambridge Analytica-Facebook situation shows that placing the burden on individuals to protect themselves is unreasonable given the proliferation of increasingly complex data-collection and -sharing arrangements.

[14] https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

Second, the bill proposed a new right called "respect for context": This new protection establishes an enforceable expectation that companies will collect, use and disclose personal data in ways that are consistent with the *context* in which consumers first provided that data. Simply put, respect for context establishes the right not to be surprised by how one's personal data is used.

Applied to the Cambridge Analytica abuses, this right would have prohibited the firm from unilaterally repurposing research data for political purposes. Because the original context was academic research, individuals would have had to consent again before their data could be used for political purposes. This new right also would have precluded the wholesale harvesting of personal data of friends of those who consented to be research subjects. Most importantly, the legislation would have put the burden of protecting individual rights on both Cambridge Analytica and Facebook, as opposed to innocent users.

Respect for context does not mean shutting down all uses of personal data or shutting off innovative uses of the "social graph" (the data that represents users' relationships in online platforms). Consider the difference between Cambridge Analytica's use of Facebook data and how information was used by the Obama 2012 reelection campaign app. During the 2012 presidential campaign Barack Obama supporters were invited to install a Facebook app that was given access to the user's friend list. Upon the app gaining access to the friend list, users were given the ability to send personalized messages to any or all of their friends, inviting them to events or sharing campaign literature. In other words, the individual, not the campaign, communicated with users' friends.. Enabling one individual user to communicate directly with his or her friends was respectful of the context in which data was collected. Users expected that they would hear from their friends. It's a social network after all. Individuals understandably did not, however, expect that their data would be gathered and assessed merely because they were friends with someone who agreed to be part of a research study. No one would expect that all of their personal data would wind up with an unknown commercial entity to whom the researcher sold their information.

Ensuring respect for privacy context is vital not just for individual rights but also because it is the bedrock of human community. If people can't control how they relate to others, there can be no genuine community, only blinding transparency from which people will seek to hide. Threats to privacy in cities equipped with pervasive sensors and analytics may chill the very communal vitality that makes our cities hubs of cultural and economic innovation. Homes with intrusive always-on sensors unrestrained by privacy rules could subtly but seriously change the intimate dynamics of our home life. And our political landscape may be altered for the worse if person data is harvested for clandestine targeting purposes.

Privacy protection faces challenges of substance and of enforcement. As recent reports show, privacy enforcers in Facebook's largest markets in the U.S. and in Europe failed to detect, deter and punish these egregious violations. It is not sufficient simply to enact privacy principles in law, as Europe has done, nor even to have great enforcement technique, which the Federal Trade Commission does. Aggressive fines would help (Europe's looming digital standards allow penalties of up to 4 percent of firms' annual revenue to be assessed), but more is needed. Centralized regulators, including the FTC and data protection authorities in the EU member states, are struggling to keep up with the use of personal data all over the commercial world. In the United States, FTC privacy enforcement historically has been limited to advertising and profiling for marketing purposes. Now the commission is called upon to address data used in home-based internet-of-things networks, face recognition and autonomous vehicles, to name a few emerging fields. The FTC's enforcement arsenal should be supplemented with rights for citizens whose privacy is infringed. This would also engage the investigation and litigation energy of the plaintiffs bar.

As a means of dealing with the scale of personal data being used, the Consumer Privacy Bill of Rights would have encouraged the development of enforceable industry codes of conduct, or industry-developed rules that implement the legislative requirements for a given sector. After a code is developed and presented to the FTC, the commission determines whether or not it complies with the consumer rights in the law. If the FTC approved the code, it would then constitute a safe harbor against FTC enforcement for members of that industry that complied with the code. For members of the industry group that accept the code but do not comply, these serve as the basis for enforceable promises that, when violated, would trigger FTC enforcement and penalties. This co-regulatory mechanism has to be implemented carefully, lest industry be allowed to water down the rules in the statute, a legitimate worry some privacy advocates have expressed.

B. Keep it simple

Policy makers approaching the challenge of legislating about privacy will have a directional choice to make. They can chose a model from the technocratic bag of tricks developed by Congress to address large industries such as was done with the Telecommunications Act of 1996.[15] That Act runs over 120 pages and took more than five years to pass. It would be understandable if Congress went this direction -- a exhaustive statute can carefully address all of the edge cases of privacy and provide the protections, justified or not, for particular industries that might get ensnared in the laws traps.

[15] Public Law 104-104 (1996)

Or, Congress could follow the example of laws that have regulated broad swaths of the economy with remarkable simplicity and technological neutrality. The Copyright Act, responsible for regulating rights of authors and content providers, is remarkably simple given the complexity of the market. The operative part of the Act is really just the first nine sections[16] and fills less than 20 pages. The antitrust laws are equally brief. The Sherman Antitrust Act[17] is only seven sections filling a few pages, and the other key competition statutes are similarly brief. Indeed, the portion of the Federal Trade Commission Act the governs more or less the whole of consumer protection, along with privacy and security, today is just one brief section filling less than a page.[18]

Why does size matter? First, we can see the the US legal system has done very well governing complex parts of the economy with simple legislative rules that are subsequently enforced by expert agencies (the FTC or Department of Justice) subject to interpretation and control over the scope of enforcement authority by the courts. This builds on the best of our common law tradition of making progress case-by-case, in response to real social and technical circumstances, as opposed to trying to predict the future. When Congress tried to dictate in exhaustive detail how broad principles are to be enforced and how the authority of enforcement agencies are to be used, the process can easily become inflexible and bogged down in the uncertainty of cycles of appeals of administrative rulemaking procedures.

C. Don't try GDPR here

Finally, if there is one thing that the US ought *not* to do in the name of privacy it is to try to implement something like EU General Data Protection Regulation (GDRP). The GDPR is a laudable legislative effort. And, many of the principles enshrined in the GDPR are actually quite similar to those in US privacy laws. However, there are major differences that make the model inapplicable to the US legal system. From a jurisdictional perspective, it reaches to cover nearly all personal data processing in the EU legal framework, including areas such as banking, consumer credit, health information, and many other industries for which the United States already has sector-specific privacy rules in place. Structurally it is a top-down, highly-detailed set of rules for handling personal data, premised on the existence of a hierarchical set of independent Data Protection Authorities in each EU country, under the control of a central authority in Brussels. All of this operates under the oversight of the EU constitutional court, enforcing and interpreting EU-wide fundamental rights guarantees of both privacy and data protection.

[16] 18 USC §§ 101-107.
[17] 15 U.S.C. §§ 1–7
[18] 15 U.S.C. § 45.

Enacting something like the GDPR would require a number of feats of political and legislative contortion that are virtually guaranteed to fail. First, because the GDPR covers nearly all commercial and much governmental use of personal data, the US Congress would have to repeal most Federal privacy laws and replace them with a single set of legal rules. I believe that the US's sector-specific privacy rules are actually a strength, and an advantage to both citizens and industry. Having sector-specific rules written by legislators with subject-matter expertise, and enforced by those who know the industry well is a real benefit. Scrapping these sector-specific rules would leave us with weakened enforcement authority where expertise is needed. What's more, getting a number committees in the US Congress to give up their authority over privacy rules in their jurisdiction in favor of some other committee seems politically nearly impossible. Second, as the GDPR requires a field of new, independent enforcement agencies linked to a constitutional court, the US would likely have to enact a constitutional right of privacy to actually be faithful to the GDPR model.

None of this critique is to suggest that there is anything wrong with the GDPR for Europe. Their parliamentary and executive branches went through extensive democratic debate on the matter and reached a result that is true to the EU civil law system. In the United States, we have to come to our own view of how to protect privacy. We can be confident, because the US and Europe have a long traditional of privacy policy development together.[19] European law requires that its citizens' personal data only be transferred to third countries with 'adequate' data privacy law. If the US develops new privacy law in good faith, we can be confident that the result will have enough in common with the EU that we will be able to work together toward a common, trans-Atlantic standard that supports the flow of personal data between the two regions[20].

V. Conclusion

In the coming years, the United States will continue to face numerous privacy challenges. True to our nature as a federal system, valuing the diversity and bottom-up nature of our legal system, we will likely see efforts to address privacy in many state legislatures and in courts around the country. As the last year has shown, questions are privacy are truly national, implicating many of our core constitutional and political values. So sooner or later, we will have to face these challenges together as a nation, under the banner of a unified national conversation. I've laid out both the reasons to worry about privacy risk and the threats of failing

[19] Weitzner, "Privacy for a Global Information Society: High Standards, Global Cooperation, and Flexibility for the Future." in Hijmans, H., & Kranenborg, H. (2014). Data protection anno 2014: How to restore trust. Contributions in honour of Peter Hustinx, European data protection supervisor (2004–2014), Intersentia, 237-252.
[20] Abramatic, J-F., B. Bellamy, M. E. Callahan, F. Cate, P. van Eecke, N. A. N. M. van Eijk, E. Guild, Weitzner, D. J. "Privacy Bridges: EU and US Privacy Experts In Search of Transatlantic Privacy Solutions." (2015)

to act in a coordinated manner. The legal community, especially those advising companies, governments and other institutions that are entrusted with more and more personal information, will have a critical role in that dialogue. So I thank you for the chance to raise these issues with you and look forward to your questions.

Weitzner is Founding Director of the MIT Internet Policy Research Initiative and Principal Research Scientist at MIT's Computer Science and Artificial Intelligence Lab. From 2011-12 he was White House Deputy Chief Technology Officer for Internet Policy where his work included online privacy. He can found on Twitter at @djweitzner.