Statement of Nuala O'Connor, President and CEO
Center for Democracy & Technology

before the
United States Senate Committee on Commerce, Science, and Transportation

Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act

October 10, 2018

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to testify about the state of consumer privacy law, lessons learned from recent state law efforts, and opportunities for a federal privacy law. CDT is a nonpartisan, nonprofit 501(c)(3) charitable organization dedicated to advancing the rights of the individual in the digital world. CDT was founded in 1994 by pioneering internet advocates Jerry Berman, Janlori Goldman, Jonah Seiger, Deirdre Mulligan, and Danny Weitzner. CDT's founding coincides with the dawn of the commercial internet, and CDT continues to focus on the critical issues of protecting and elevating individual privacy, freedom of expression, and freedom from surveillance, while also seeking to advance innovation and preserve a global, open Internet. CDT has offices in Washington, D.C., and Brussels, and is funded by foundation grants for research and writing, corporate donations for general operating and program support, and individual program and event donations.[1]

I have been honored to serve CDT and the public interest for the past five years as President and CEO. My viewpoints today are not only informed by the research, analysis, and advocacy of the lawyers, policy analysts and technologists at the Center for Democracy & Technology, but also by almost 30 years of professional experience, much in the privacy and

[1] All donations over $1,000 are disclosed in our annual report and are available online at: https://cdt.org/financials/.

data realm. While in the private practice of law, I counseled some of the internet's earliest commercial websites; I have served as a corporate privacy leader at General Electric, Amazon, and DoubleClick; and was honored to have served as the chief privacy officer for two federal government agencies - the U.S. Department of Commerce and the U.S. Department of Homeland Security. When I was appointed by President George W. Bush as the first chief privacy officer at the Department of Homeland Security under Secretary Tom Ridge, I was the first statutorily mandated CPO in the federal service.

CDT submits this testimony and engages in this work informed by the underlying belief that internet-enabled technologies have the power to change lives for the better. And yet, nearly 25 years on from the dawn of the commercial internet, it is appropriate that we take stock of where we are, and where we are going. As with many new technological advancements and emerging business models, we have seen exuberance and abundance, and we have seen missteps and unintended consequences. International bodies and U.S. states have responded by enacting new laws, and it is time for the U.S. federal government to pass omnibus federal privacy legislation to protect individual digital rights and human dignity, and to provide certainty, stability, and clarity to consumers and companies in the digital world.

The Need for Federal Legislation

The U.S. privacy regime today does not efficiently or seamlessly protect and secure Americans' personal information. Instead of one comprehensive set of rules to protect data throughout the digital ecosystem, we have a patchwork of sectoral laws with varying protections depending on the type of data or the entity that processes the information. While this approach may have made sense decades ago, it now leaves a significant amount of our personal information - including some highly sensitive or intimate data and data inferences - unprotected.

Our current legal structure on personal data simply does not reflect the reality that the internet and connected services and devices have been seamlessly integrated into every facet of our society. Our schools, workplaces, homes, automobiles, and personal devices regularly create and collect, and, increasingly, infer, intimate information about us. Everywhere we go, in the real world or online, we leave a trail of digital breadcrumbs that reveal who we know, what we believe, and how we behave. Overwhelmingly, this data falls in the gaps between regulated sectors.

The lack of of an overarching privacy law has resulted in the regular collection and use of data in ways that are unavoidable, have surprised users, and resulted in real-world harm. A

constant stream of discoveries shows how this data can be repurposed for wholly unrelated uses or used in discriminatory ways:

- Madison Square Garden deployed facial recognition technology purportedly for security purposes, while vendors and team representatives said the system was most useful for customer engagement and marketing.[2]
- Application developer Alphonso created over 200 games, including ones targeted at children, that turn on a phone's microphone solely for marketing purposes.[3]
- Office Max mailed an advertisement to a Chicago man with "Daughter Killed In Car Crash" in the addressee line.[4]
- Facebook permitted housing advertisements to be obscured from parents, disabled people, and other groups protected by civil rights laws.[5]

The lack of an overarching privacy law has also resulted in absurd legal outcomes. Consider personal health information; whether this information is protected by federal privacy law depends on who possesses it. Healthcare and health insurance providers are required to keep health information confidential under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), but no one else is, including health and fitness device and app developers that are regularly collecting some of the same information.[6] Americans' privacy interest in health information does not diminish because it is processed by an app developer instead of a healthcare provider.

---

[2] Kevin Draper, Madison Square Garden Has Used Face-Scanning Technology on Customers, NYT, Mar. 13, 2018.
[3] Sapna Maheshwari, That Game on Your Phone May Be Tracking What You Watch on TV, NYT, Dec. 28, 2017, https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html.
[4] Nestia Kwan, OfficeMax Sends Letter to "Daughter Killed In Car Crash," nbcchicago.com, Jan 14, 2017, https://www.nbcchicago.com/news/local/OfficeMax-Sends-Letter-to-Daughter-Killed-in-Car-Crash-240941291.html.
[5] Brakkton Booker, HUD Hits Facebook for Allowing Housing Discrimination, NPR, Aug. 19, 2018, https://www.npr.org/2018/08/19/640002304/hud-hits-facebook-for-allowing-housing-discrimination.
[6] HHS, Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA 6, https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf. This is an imminent concern, as the Centers for Medicare and Medicaid Services are advancing the Blue Button 2.0 Standard, which would make more healthcare information available to developers.

While the Federal Trade Commission's ability to police unfair and deceptive practices provide a backstop, large gaps in policies around access, security, and privacy exist, which confuse both individual consumers and businesses. Because the FTC is prohibited from using traditional rulemaking processes, the agency has created a "common law" of privacy and security through its enforcement actions.[7] Creating proactive privacy rights through a process-of-elimination approach will not be able to keep up with advances in technology and the explosion of device and app manufacturers.

Without legislation, we may be stuck in a framework based on notice and consent for the foreseeable future.[8] "Notice" is provided through a presentation of legal terms and conditions, while "consent" is any action that signifies the acceptance of those terms. This model encourages companies to write permissive privacy policies and enticing users agree to data collection and use by checking (or not unchecking) a box. This model persists despite the fact that few individuals have the time to read privacy notices,[9] and it is difficult, if not impossible, to understand what they say even if they are read.[10]

Even if an individual wants to make informed decisions about the collection, use, and sharing of their data, user interfaces can be designed to tip the scales in favor of disclosing more personal information. For example, the FTC reached a settlement with PayPal in February after its Venmo service misled users about the extent to which they could control the privacy of their financial transactions.[11] Users' transactions could be displayed on Venmo's public feed even if users set their default audience to private. In the case of the Cambridge Analytica disclosure, users purportedly consented to disclosing information by filling out a quiz, but had no way of foreseeing how that information would be used.[12]

---

[7] Daniel Solove and Woody Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia L. Rev. 583, (2014).

[8] See, e.g., Fred Cate, The Failure of Fair Information Practice Principles, in THE FAILURE OF FAIR INFORMATION PRACTICE PRINCIPLES 342, 351 (Jane Winn ed., 2006); and Solon Barocas & Helen Nissenbaum, On Notice: The Trouble with Notice and Consent, Proceedings of the Engaging Data Forum, (2009).

[9] Aleecia McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: A Journal of Law and Policy 543, (2008).

[10] Joel Reidenberg, Presentation, Putting Disclosures to the Test (2016), available at https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test.

[11] Press release, FTC, Feb. 28, 2018, https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

[12] Kevin Granville, Facebook and Cabridge Analytica: What you Neeed to Know as Fallout Widens, NYT, Mar. 19, 2018, https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

Beyond any one privacy decision, the sheer number of privacy policies, notices, and settings or opt-outs one would have to navigate strain individuals' cognitive and temporal limitations. It is one thing to ask an individual to manage the privacy settings on their mobile phone; it is another to tell them they must do the same management for each application, social network, and connected device they use. Dozens of different data brokers operate different opt-outs.[13] Further, people operate under woefully incorrect assumptions about how their privacy is protected.[14] Privacy self-management alone is neither scalable or practical for the individual. Burdening the individual consumer or citizen with more and more minute choice and decisionmaking, absent some reasonable boundaries, will not provide the systemic changes we need.[15]

It is important to note that privacy harms can still emerge separate and distinct from any single individual's choice or consent and despite an individual's attempts to exercise a choice. A service's data practices can harm individuals who are not even users of the service. This spring, for example, the fitness tracking app Strava displayed a heatmap of users' runs that revealed the locations and outlines of military and covert activity that could be used to identify interesting individuals, and track them to other sensitive or secretive locations.[16] The harms stemming from this type of disclosure can reach people who never used the app and thus never had the option to "consent" to Strava's data policies.

CDT is not the only entity to critique notice and consent as the predominant privacy control in U.S. law. Just last month, the National Telecommunications and Information Administration (NTIA) acknowledged the shortcomings of the notice-and-consent model. The administration's request for comment on privacy noted that "relying on user intervention may be insufficient to manage privacy risks."[17] Of course, constructing a new framework is complicated and will only happen by way of statute. It is time to rebuild that trust by providing a baseline of protection for Americans' personal information that is uniform across sectors, that

---

[13] Yael Grauer, Here's a Long List of Data Broker Sites and How to Opt-Out of Them, Motherboard (Mar. 27, 2018), https://motherboard.vice.com/en_us/article/ne9b3z/how-to-get-off-data-broker-and-people-search-sites-pipl-spokeo.

[14] Joseph Turow, Let's Retire the Phrase 'Privacy Policy', N.Y. Times (Aug. 20, 2018), https://www.nytimes.com/2018/08/20/opinion/20Turow.html.

[15] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).

[16] Jeremy Hsu, The Strava Heatmap and the End of Secrets, Wired, Jan. 29, 2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

[17] National Telecommunications and Information Administration, Request for Comments on Developing the Administration's Approach to Consumer Privacy, Sept. 25, 2018, https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.

follows the data as it changes hands, and that places clear limits on the collection and use of personal information.

What Legislation Should Include

Instead of relying primarily on privacy policies and other transparency mechanisms, Congress should create an explicit and targeted baseline level of privacy protection for individuals. As discussed below, legislation should enshrine basic individual rights with respect to personal information; prohibit unfair data processing; deter discriminatory activity and give meaningful authority to the FTC and state attorneys general to enforce the law.[18]

Individual Rights in Data

A federal law must include basic rights for individuals to access, and in some instances, correct their personal data held by companies; individuals should also have the ability to easily delete or move information out of services.[19] It should also enshrine the right to know how and with whom personal data is shared. These overarching rights are relatively noncontroversial. Companies must already extend them to their EU users under the General Data Protection Regulation (GDPR), and elements of these rights are also at the core of the recent California Consumer Privacy Act. They have been recognized by the U.S. government and international bodies for decades, albeit in voluntary form.[20] With appropriate, tailored exceptions, these provisions can be crafted in a way that does not unduly burden companies' business practices or interfere with the provision of services.

Where feasible, these rights should apply not only to data that users have shared with a company but also to information that a company has observed or inferred about users, such as their location, web browsing information, and advertising categories they have been placed in. Inferences can be more sensitive and relevant than the data a user directly discloses to a company, are often invisible to the user, and can be the basis for decisions that have significant effects on people's lives. A 2013 report by this committee found that data brokers created and sold consumer profiles identifying people as "Rural and Barely Making It," "Ethnic Second-City

[18] While we do not address transparency per se in this statement, we assume that any legislation will include such provisions and are available to discuss possibilities in detail with Congressional offices.

[19] https://eu.usatoday.com/story/tech/columnist/2017/11/12/web-companies-should-make-easier-make-your-data-portable-ftcs-mcsweeny/856814001/

[20] Robert Gellman, Fair Information Practices: A History, 2012, https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

Strugglers," and "Retiring on Empty: Singles." This information can be used to target vulnerable consumers with potentially harmful offers, such as payday loans.

Federal legislation should enshrine rights like access, deletion, and portability, but it cannot stop there. While these rights give individuals control over their data in some sense, they are not a substitute for the systemic changes we need to see in data collection and use.

Declaration that certain data practices are presumptively unfair

Users are often comfortable providing the data required to make a service work, but in providing that information, they are often asked to consent to long, vague lists of other ways in which that data may be used or shared in the future. These future uses are often couched in terms such as research, improving services, or making relevant recommendations, and the precise nature of these secondary uses are often difficult for users to foresee.

While data provided in the context of a commercial transaction can often be considered part of an ongoing business relationship, and used in the context of future transactions between the parties, there are some types of data and some processing practices that are so sensitive that they should be permitted only to provide a user the service they requested, and prohibited from entering the opaque and unaccountable market of secondary uses. These practices could include the collection and processing of precise location information, the use of biometric information to identify individuals, and the use of healthcare information or children's information for targeted marketing. For example, if a user opts-in to a feature that allows her to unlock her phone with her face, her unique face data should be used only to provide that feature, and perhaps improve performance of that feature. But the data should not be used, for example, to unexpectedly recognize and tag her in photos or for other secondary purposes - without her specific, separate choice to engage in that service. Repurposing these types of data for a purpose far afield from the primary transaction without independent indication of consent should generally be considered an unfair practice under Section 5 of the FTC Act.

Rules to prevent discriminatory effects

Independent entities have attempted to study whether online advertising can facilitate the violation of long-standing civil rights laws.[21] These studies have determined that in some cases, advertisers are able to prevent parents, the disabled, and other protected classes from

[21] See Booker, note 5; Julia Angwin, et. al, Dozens of Companies are Using FAcebook to Exclude Older Workers From Jobs, Dec. 20, 2017, https://www.propublica.org/article/facebook-ads-age-discrimination-targeting.

receiving advertisements for housing or employment. This has prompted some platforms to reevaluate and reform their systems.[22] Because online advertising is ephemeral, individuals and government agencies may face unique challenges in defending civil rights. To that end, a data privacy statute should focus on the potential for opaque discriminatory effects based on data decisioning, and should articulate a non-discrimination standard. The FTC should be directed to write rules to mitigate the ways new advertising models disproportionately disadvantage protected classes.

Meaningful enforcement mechanisms

Affirmative individual rights and data collection and use restrictions may ultimately be meaningless absent strong enforcement. While we believe that the Federal Trade Commission has been effective as the country's "top privacy cop," it is also an agency that desperately needs more resources. Funding for the agency has fallen five percent since 2010, and its resources are strained.[23] In 2015, the FTC had only 57 full time staff working in the Department of Privacy and Identity Protection, with additional staff working in enforcement and other areas that could touch on privacy.[24] In additional to more FTC funding, federal legislation must include two new statutory enforcement mechanisms.

First, the FTC must be given the ability to extract meaningful fines from companies that violate individuals' privacy. Because much of the Commission's existing privacy enforcement falls under Section 5 of the FTC Act, it does not possess original fining authority and companies are functionally afforded one free "bite at the apple" regardless of the intent or impact of a privacy practice.[25] At present, before a company may be fined for violating individuals' privacy, it must first agree to and be placed under a consent decree, and then subsequently violate that agreement.

---

[22] Facebook Agrees to Prevent Discriminatory Advertising, LAT, July 24, 2018, at http://www.latimes.com/business/technology/la-fi-tn-facebook-discrimination-advertising-20180724-story.html;

[23] David McCabe, Mergers are spiking, but antitrust cop funding isn't, AXIOS, May 7, 2018, https://www.axios.com/antitrust-doj-ftc-funding-2f69ed8c-b486-4a08-ab57-d3535ae43b52.html; seel also https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/?utm_term=.c6c304221989

[24] https://www.ftc.gov/system/files/documents/reports/fy-2016-congressional-budget-justification/2016-cbj.pdf

[25] Dissenting Statement of Commissioner J. Thomas Rosch, In the Matter of Google Inc., FTC Docket No. C-4336 (Aug. 9, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googleroschstatement.pdf.

Relying solely on consent decree enforcement has been inadequate to protect user privacy. The penalties for violating a decree may be so insignificant that they do not have the intended deterrent effect. For instance, when Google agreed to pay a $22.5 million penalty for violating the 34 terms of its consent order in 2012, this was approximately five hours worth of Google's revenue at the time.[26] Additionally, Facebook has been under a consent decree throughout the entire duration of its dealing with Cambridge Analytica, as well as its merger of data between its Facebook platform and WhatsApp.[27]

Second, state attorneys general must be granted the authority to enforce the federal law on behalf of their citizens. State attorneys general have been enforcing their own state consumer privacy laws for decades, first under state unfair and deceptive practice laws and more recently under state statutes targeted at specific sectors or types of data.[28] Employing their expertise will be necessary for a new federal privacy law to work. A law with the scope we are proposing will bring large numbers of previously unregulated entities into a proactive regime of new privacy and security requirements. There will simply be no way for a single agency like the FTC to absorb this magnitude of new responsibilities.

Additionally, each state has a unique combination of demographics, prevailing industries, and even privacy values, and many privacy or security failures will not affect them equally. State attorneys general must be able to defend their constituents' interest even if the privacy or security practice does not rise to the level of a national enforcement priority. Arguably, local enforcement is best for small businesses. A state attorney general's proximity to a small business will provide context that will help scope enforcement in a way that is reasonable.

Conclusion

The existing patchwork of privacy laws in the United States has not served Americans well, and as connected technologies become even more ubiquitous, our disjointed privacy approach will only lead to more unintended consequences and harms. We risk further ceding our leadership role on data-driven innovation if we do not act to pass baseline privacy

---

[26] Id. Commissioner Rosch noted that a $22.5 million fine "represents a de minimis amount of Google's profit or revenues."

[27] Laura Sydell, FTC Confirms It's Investigating Facebook for Possible Privacy Violations, NPR (March 26, 2018), https://www.npr.org/sections/thetwo-way/2018/03/26/597135373/ftc-confirms-its-investigating-facebook-for-possible-privacy-violations.

[28] Danielle Keats Citron, The Privacy Policy Making of State Attorneys General, 92 Notre Dame L. Rev. 747 (2016), https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4693&context=ndlr.

legislation. Effective privacy legislation will shift the balance of power and autonomy back to individual consumers, while providing a more certain and stable regulatory landscape that can accelerate innovation in the future. The time is now to restore the digital dignity for all Americans. Congress must show their leadership and pass a comprehensive privacy law for this country.