GEORGETOWN LAW
Center on Privacy & Technology

Statement of Laura Moy
Executive Director, Center on Privacy & Technology at Georgetown Law

Before the

U.S. Senate
Committee on Commerce, Science, and Transportation

Hearing on

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

Wednesday, October 10, 2018

For more information, contact Laura Moy at laura.moy@georgetown.edu.

Introduction and Summary

Chairman Thune, Ranking Member Nelson, and Members of the Committee, thank you for inviting me here today. I am Laura Moy, executive director of the Center on Privacy & Technology at Georgetown Law. I appreciate the opportunity to testify on consumer privacy.

It feels significant to come before this institution in such an electrically charged time, and it feels important to speak truth in that context. So I wanted to start by explaining why I am here. I am not here today because I am worried about private information being made public. This is not, for me, just about the classic "right to be left alone."

This is about our country—and the world—grappling with the implications of unbridled data collection, storage, and use—things that give the holders and users of data more power to influence society than we could have imagined before the digital era. This is about confronting the ways in which the data-driven economy is contributing to extreme wealth disparity, extreme political polarization, extreme race- and class-based tension, and extreme information manipulation. We need to come together to rein in the problematic ways in which Americans' data is being collected and stored without meaningful limitations, and used in ways that harm not only individuals, but our broader society.

As this Committee considers what form those solutions might take, I offer a handful of recommendations that I hope to highlight in my testimony today:

- **First, there are appropriate and inappropriate collections and uses of Americans' information.** To foster data fairness, baseline obligations should attach to all collections and uses of consumer data. And some applications for Americans' data should simply be off-limits. Chief among these is discrimination—information should not be used to selectively deny access to—or awareness of—critical opportunities in housing, education, finance, employment, and healthcare.

- **Second, privacy protections should be strongly enforced by an expert agency.** Standards are only as strong as their enforcement, so whatever standards this legislature crafts, they should be enforceable by an expert agency that has civil penalty authority and sufficient staff, resources, and motivation to get its job done.

- **Third, privacy protections should also be enforced by state attorneys general.** Federal agencies cannot possibly hope to police the entire digital ecosystem. State attorneys general are already doing extensive and excellent work on privacy and data security, and they must be empowered to continue to do that good work under any new legislation.

- **Fourth, privacy and data security protections should be forward-looking and flexible.** As the technological landscape changes, privacy and data security standards must constantly be updated. State legislatures are already doing this, operating as the "laboratories of democracy" they are supposed to be, and federal law should not hamstring states' ability to continue to do this work. Any new standards on privacy and data-security standards should also include rulemaking authority for an expert agency that is able to keep abreast of and respond to shifting threats as technology advances.

- **Fifth, protections for Americans' private information should take into account the context in which information is shared.** There are different types of actors on the internet with different roles to play, different relationships with and commitments to users, different competition environments, and different abilities to solve problems. Any new privacy and data security standards should be tailored to ensure that Americans continue to benefit from heightened privacy standards in contexts in which choices are limited and privacy expectations are higher.

- **Sixth, Congress should not eliminate existing protections for Americans' information.** This should go without saying, but as Congress considers establishing new privacy and data security protections for Americans' private information, what it should *not* do is eliminate existing protections that are already benefiting Americans in state or other federal laws.

1. We need to broaden the conversation on privacy

"Privacy" has many definitions. For example, it could refer to the right to keep private information from being exposed to the public, the right to control information about oneself, the right to be left alone, the right to ensure that information is used and shared in a way that is consistent with norms and expectations, or the right to prevent information from being

transferred to those who would use it to do harm. It is all of these things, but in the networked era it is more.

When we talk about privacy today, we should also be thinking about the right to ensure that our information is not used in ways not only that harm ourselves, but that harm society as a whole. For example, beyond subjecting individual users to specific uses and transfers that they find objectionable, information uses and misuses may harm society by:

- Chilling both adoption and free and open use of the internet. The FCC concluded in the 2010 *National Broadband Plan* that concerns about online privacy and security "may limit [consumers'] adoption or use of broadband."[1] More recently, NTIA reported that 45% of households limited their online activities because of privacy and security concerns.[2]

- Undermining trust in the digital environment. When information is not sufficiently protected, Americans cannot fully trust the digital environment. But as privacy scholars writing on the importance of trust as an element of privacy policymaking have explained, "trust drives commerce and it creates the conditions for intimacy and free expression. If we want to flourish as humans, we must be able to trust each other."[3]

- Supporting the dissemination of propaganda, misinformation, and disinformation. Americans' data may be used to generate and target false information, including state-sponsored propaganda, careless or low-quality reporting, and false information designed and intended to

---

[1] FCC, *Connecting America: The National Broadband Plan* 17 (2010), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[2] Rafi Goldberg, NTIA, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities* (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[3] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 Stan. Tech. L. Rev. 431, 456 (2016).

undermine democracy.[4] As false information proliferates, Americans are rapidly losing trust in journalism.

- Amplifying hate speech. Americans' data may also be used to make the distribution of hateful and racist rhetoric and calls to violence more efficient.[5]

- Driving political polarization. Americans' data may also be used to drive content distribution platforms that are more likely to promote hyper-partisan content, which in turn may exacerbate political polarization. As one prominent legal scholar has written, "Self-insulation and personalization are solutions to some genuine problems, but they also spread falsehoods, and promote polarization and fragmentation."[6]

- Damaging public health. Digital sites and services often use users' data to inform design choices that will increase user engagement, including by intentionally designing products to be addictive and inescapable.[7] This can lead to a cascade of other problems, including

---

[4] David McCabe, *Facebook Finds New Coordinated Political Disinformation Campaign*, Axios, July 31, 2018, https://www.axios.com/facebook-finds-misinformation-campaign-4c5910b3-021a-45b7-b75c-b1ac80cbce49.html; Dipayan Ghosh & Ben Scott, *Disinformation Is Becoming Unstoppable*, Time, Jan. 24, 2018; April Glaser & Will Oremus, *The Shape of Mis- and Disinformation*, Slate, July 26, 2018, https://slate.com/technology/2018/07/claire-wardle-speaks-to-if-then-about-how-disinformation-spreads-on-social-media.html; Alice Marwick & Rebecca Lewis, *Media Manipulation and Disinformation Online* (2017), https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

[5] *See* Ariana Tobin, Madeleine Varner, & Julia Angwin, *Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up*, ProPublica, Dec. 28, 2017, https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes; Swathi Shanmugasundaram, Southern Poverty Law Center, *The Persistence of Anti-Muslim Hate on Facebook* (May 5, 2018), https://www.splcenter.org/hatewatch/2018/05/05/persistence-anti-muslim-hate-facebook.

[6] Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* at 5 (2017).

[7] Center for Humane Technology, The Problem, http://humanetech.com/problem/ (last visited Oct. 7, 2018) (explaining that operators of online

heightened rates of depression, suicide, and sleep deprivation among young people.[8]

We should be thinking of these problems as we consider how best to approach data legislation in the 21st century. It may not be possible to solve all of these problems at once, but any proposed legislative solution to one problem should be scrutinized to ensure that it does not inadvertently make these problems worse, or hamper the ability of states or enforcement agencies to innovate additional approaches to some of these problems moving forward.

2. We must do better on privacy

We must do better on privacy. Americans consistently are asking for policymakers to step in. 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies, and 68% believe current laws are not good enough in protecting people's privacy online. In response to one 2015 survey, 80% of respondents were "concerned" or "very concerned" when asked about their online privacy.[9] For years, consumers have been expressing concern and even anger about the way their personal information is collected and used without their control,

---

services competing for users' attention are constantly learning how better to "hook" their users, and designing products intentionally to addict users).

[8] Recent studies have linked the use of platforms like Facebook, Snapchat, and Instagram to depressive symptoms in young adults caused by negatively comparing oneself to others on social media platforms. Brian A. Feinstein, et al., *Negative Social Comparison on Facebook and Depressive Symptoms: Rumination as a Mechanism*, 2 Psych. Pop. Media Culture 161 (2013). http://psycnet.apa.org/record/2013-25137-002. Experts have also found that teens who spend three hours a day or more on electronic devices are 35 percent more likely to have a risk factor for suicide and 28 percent more likely to get less than seven hours of sleep. Jean M. Twenge, *Have Smartphones Destroyed a Generation?*, The Atlantic, Sept. 2017, https://www.theatlantic.com/magazine/archive/2017/09/has-the-smartphone-destroyed-a-generation/534198/.

[9] Freedman Consulting, *Poll Finds Strong Support for Expanding Online Privacy Protections and Internet Access* (Nov. 23, 2015), *available at* https://www.freedmanconsulting.com/documents/PrivacyandAccessResearchFindings_151123.pdf.

consent, or even knowledge.[10] Americans feel powerless to regain control over their privacy—in the modern era, Internet access is necessary for employment, education, access to housing, and full participation in economic and civic life.

In the absence of robust regulation, although providers of online sites and services often engage in ongoing conversations with civil rights, civil liberties, and public interest groups, they nevertheless have repeatedly failed to respect and protect data relating to millions—and at times billions—of users. For example, despite repeated assurances to regulators, the public, and advocates that it would protect consumer privacy, Facebook has revealed breach after massive breach, including when, less than two weeks ago, it announced a breach that may have affected up to 90 million users.[11] Last year data miners, chief among them Cambridge Analytica, successfully used Facebook's platform to learn private information about many more than 87 million users.[12] And Facebook also recently revealed that "malicious actors" had exploited search tools on its platform to harvest profile details of most of its two billion users.[13] Despite Google's past promises to stop scanning the inboxes of Gmail users for information to target marketing, it was reported in July that the company continues to let hundreds of third-party companies

---

[10] Lee Rainie & Maeve Duggan, Pew Research Center, *Privacy and Information Sharing* 2 (Jan. 14, 2016), http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf ("In online focus groups and in open-ended responses to a nationally representative online survey, many people expressed concerns about the safety and security of their personal data in light of numerous high-profile data breaches. They also regularly expressed anger about the barrage of unsolicited emails, phone calls, customized ads or other contacts that inevitably arises when they elect to share some information about themselves.").

[11] Louise Matsakis & Issie Lapowsky, *Everything We Know About Facebook's Massive Security Breach*, WIRED, Sept. 28, 2018, https://www.wired.com/story/facebook-security-breach-50-million-accounts/.

[12] Alex Hern, *Far More than 87m Facebook Users Had Data Compromised, MPs Told*, The Guardian, Apr. 17, 2018, https://www.theguardian.com/uk-news/2018/apr/17/facebook-users-data-compromised-far-more-than-87m-mps-told-cambridge-analytica.

[13] Craig Timberg, Tony Romm, & Elizabeth Dwoskin, *Facebook: 'Malicious Actors' Abused Its Search Tools to Collect Data on Most of Its Two Billion Users*, The Independent, Apr. 5, 2018, https://www.independent.co.uk/news/world/americas/facebook-hackers-personal-data-collection-users-cambridge-analytica-trump-mark-zuckerberg-latest-a8289816.html

scan the inboxes of millions of Gmail users, doing little to police what those third parties do with users' information.[14] Google also revealed that it still tracks users' location through use of its services even after users have disabled the "Location History" feature.[15] And the past several months have seen major security breaches affecting, among others, Orbitz,[16] Under Armour,[17] Ticketfly,[18] and British Airways.[19]

Consumers are outraged and consistently are calling for greater oversight and accountability. Consumers should be able to trust that when they go online, their information will not be used to harm them.

3. Recommendations for the Committee as it considers how to address privacy

It is in this context—when Americans are increasingly concerned about privacy, and when the stakes are higher than ever—that this Committee is grappling with these many complex and important issues. Now is not the time to be shy about stepping in. "Light-touch" regulation has already been tried, and it has led us to the predicament we find ourselves in today. To

---

[14] Douglas MacMillan, *Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail*, WSJ, July 2, 2018, https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442.
[15] Chaim Gartenberg, *Google Updated its Site to Admit It Still Tracks You Even if You Turn Off Location History*, The Verge, Aug. 17, 2018, https://www.theverge.com/2018/8/17/17715166/google-location-tracking-history-weather-maps.
[16] Robert Hackett, *Expedia's Orbitz Says Data Breach Affected 880,000 Payment Cards*, Forbes, Mar. 20, 2018, http://fortune.com/2018/03/20/expedia-orbitz-data-breach-cards/.
[17] Hamza Shaban, *Under Armour Announces Data Breach Affecting 150 Million MyFitnessPal Accounts*, Wash. Post, Mar. 29, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/under-armour-announces-data-breach-affecting-150-million-myfitnesspal-app-accounts/.
[18] Travis M. Andrews, *Ticketfly is Back Online After a Hack Exposed About 27 Million Accounts. Here's What You Need to Know.*, Wash. Post, June 7, 2018, https://www.washingtonpost.com/news/arts-and-entertainment/wp/2018/06/05/ticketfly-has-been-hacked-heres-what-you-need-to-know/.
[19] Ivana Kottasová, *British Airways' Latest Tech Problem Is a Major Credit Card Hack*, CNN Business, Sept. 7, 2018, https://money.cnn.com/2018/09/07/investing/ba-hack-british-airways/index.html.

sufficiently protect Americans from harmful uses of their data, much more must be done. Below, I offer a handful of recommendations to this Committee about where to begin.

A. Recognize that there are appropriate and inappropriate collections and uses of Americans' data

It is long past time for us to move beyond a privacy framework built on the concept of notice and choice, and to recognize that there should be minimum criteria that determine when collection and use of information is appropriate, and there are also things information simply should not be used for. As the digital era advances, notice is becoming less and less meaningful—it is increasingly difficult for consumers to understand the many ways in which their information might be collected, what that information might reveal about them, and how it might be used. And "choices" often are not true choices. Americans don't feel that they have a choice about whether or not to go online—and because we all recognize that an online presence is indispensable in the 21st century, we don't want them to treat it like a choice, and avoid going online. Nor do consumers have a true choice about whether or not to share their information with a number of entities they encounter online.[20]

Beyond notice and choice, legislation should define baseline obligations that automatically attach when Americans' information is collected or used. Those obligations should be based on the familiar Fair Information Practices (FIPs) of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[21] The FIPs framework creates meaningful obligations for

---

[20] For example, consumers have no choice about whether or not to share information with a broadband provider in order to go online—and in many places in the country, there is only one choice of provider when it comes to high-speed broadband. Consumers also have virtually no choice about whether to share information with either Apple or Google when selecting an internet-enabled smartphone, virtually no choice about whether to share information with pervasive analytics and advertising networks, and, in some cases, no choice about whether or not to engage with social media platforms. In some instances, employers even require employees to have social media accounts.

[21] *See* Int'l Ass'n Privacy Professionals, *Fair Information Practices*, https://iapp.org/resources/article/fair-information-practices/ (last visited Oct.

companies that collect personal data, and rights for individuals whose personal data is collected.

Legislation should also inhibit uses of data that simply should not be allowed. Chief among these is discrimination. The information that Americans share online should not be used to selectively deny them access to—or awareness of—critical opportunities, especially things like housing, education, finance, employment, and healthcare. It should not be used to amplify hate speech. It should not be used to enable data brokers to secretly build ever-more-detailed profiles of us that they then turn around and sell, unrestricted, to the highest bidder.

At present, these impermissible uses of information are widespread. For example, on discrimination, Facebook made assurances in 2017 to tackle discriminatory advertising on its platform after facing public outrage and pressure from advocates regarding its "ethnic affinity" advertising clusters, but the Washington State Attorney General found that it was still possible to exclude people from seeing advertisements based on protected class membership.[22] Civil rights organizations are also suing Facebook for enabling landlords and real estate brokers to exclude families with children, women, and other protected classes of people from receiving housing ads,[23] as well as for gender discrimination on job ads.[24] And the systematic targeting and exclusion of communities can also be a byproduct of algorithmic content and

---

7, 2018); Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionof privacyandtransborderflowsofpersonaldata.htm (last visited Oct. 7, 2018).

[22] Sam Machkovech, *Facebook Bows to WA State to Remove "Discriminatory" Ad Filters*, Ars Technica, July 25, 2018, https://arstechnica.com/information-technology/2018/07/facebook-bows-to-wa-state-pressure-to-remove-discriminatory-ad-filters/.

[23] Nat'l Fair Housing Alliance, *Facebook Sued by Civil Rights Groups for Discrimination in Online Housing Advertisements* (Mar. 27, 2018), https:// nationalfairhousing.org/2018/03/27/facebook-sued-by-civil-rights-groups-for-discrimination-in-online-housing-advertisements/.

[24] Communications Workers of America, *CWA Sues Facebook for Gender Discrimination on Job Ads* (Sept. 20, 2018), https://www.cwa-union.org/news/ cwa-sues-facebook-for-gender-discrimination-on-job-ads.

ad distribution that optimizes for cost-effectiveness and user "engagement," which can lead to distribution that is discriminatory in impact, if not intent.[25]

Any new privacy legislation should establish standards that attach substantive legal obligations to collection and use of consumers' data, and that protect Americans from the most harmful uses of their information.

B. Privacy protections should be strongly enforced by a federal expert agency

Privacy standards are only as strong as their enforcement. Congress must empower an expert agency to vigorously enforce the law—including with the ability to fine companies for privacy and data security violations. At present, although the Federal Trade Commission is expected to enforce the privacy promises of most of the commercial sector, with few exceptions, the agency does not have the ability to levy fines for privacy and data security.[26] This is widely viewed as a challenge by agency officials; indeed, civil penalty authority has been explicitly requested by multiple FTC officials, including Chairman Simons, Commissioner Slaughter, former Commissioner Ohlhausen, former Commissioner Terrell McSweeny, and former Director of the Bureau of Consumer Protection, Jessica Rich.[27] To improve privacy and

---

[25] *See* Anja Lambrecht & Catherine E. Tucker, *Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads* (Mar. 9, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260 (finding that because younger women are an expensive demographic to show ads to, "An algorithm which simply optimizes cost-effectiveness in ad delivery will deliver ads that were intended to be gender-neutral in an apparently discriminatory way, due to crowding out."); Latanya Sweeney, *Discrimination in Online Ad Delivery*, Communications of the ACM, May 2013, at 44, https://cacm.acm.org/magazines/2013/5/163753-discrimination-in-online-ad-delivery/.

[26] There are exceptions to this rule. As the FTC explains, "If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule." FTC, *Privacy & Security Update 2016*, https://www.ftc.gov/reports/privacy-data-security-update-2016.

[27] *See, e.g., Oversight of the Federal Trade Commission: Hearing Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce* (2018) (statement of Joseph J. Simons, Chairman,

data security for consumers, the FTC—or another agency or agencies—must be given more powerful regulatory tools and stronger enforcement authority.

Agencies also need resources to do their jobs well. The FTC is a relatively small agency, and should be given additional staff and resources if it is to be expected to step up its work on privacy. The agency has a small Office of Technology Research and Investigation (OTech), but would benefit from a larger Bureau of Technology equipped to fully grapple with the challenges of advancing technology—an idea supported by numerous current and former FTC officials.[28] An agency expected to enforce the privacy and

---

Fed. Trade Commission) (calling for civil penalty authority, arguing that monetary penalties "would actually . . . cause the business to think through how it's conducting . . . its business and what it's doing in terms of security and privacy."); *id.* (statement of Rebecca Kelly Slaughter, Commissioner, Fed. Trade Comm'n) (calling for civil penalty authority); Maureen Ohlhausen, Commissioner, Fed. Trade Commission, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), transcript *available at* https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf; Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 Geo. L. Tech. Rev. 514, 529 (2018), https://www.georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-McSweeny-pp-514-30.pdf; *Opportunities and Challenges in Advancing Health Information Technology: Hearing Before the Subcomms. on Info. Tech. and Health, Benefits, and Admin. Rules of the H. Oversight and Gov't Reform Comm.* (2016) (statement of Jessica Rich, Director of the Bureau of Consumer Protection, Fed. Trade Commission).

[28] A Bureau of Technology is an idea that has been cited by Chairman Joseph Simons, Commissioner Rebecca Kelly Slaughter, former Commissioner Terrell McSweeny, and Professor David Vladeck, former Director of the Bureau of Consumer Protection. *See, e.g.*, *Oversight of the Federal Trade Commission: Hearing Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce* (2018) (statement of Joseph J. Simons, Chairman, Fed. Trade Commission) (stating that the Commission is "affirmatively evaluating whether to create a bureau of technology"); McSweeny, *supra* note 27, at 530; U.S. Fed. Trade Comm'n, *Remarks of Commissioner Rebecca Kelly Slaughter on Raising the Standard: Bringing Security and Transparency to the Internet of Things?* at 5 (July 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395854/slaughter_-_raising_the_standard_-_bringing_security_and_transparency_to_the_internet_of_things_7-26.pdf; Aaron Fluitt, Institute for Technology Law & Police at Georgetown Law, *Georgetown's David Vladeck Outlines Challenges and Opportunities for Incoming FTC Commissioners*

security obligations of companies that do business in a digital world should be vested with the necessary expertise and resources to do that job well.

Even with additional staff and resources, however, enforcement agencies may, for a variety of reasons, sometimes fail to strongly enforce privacy standards.[29] To provide an additional backstop for consumers in the event that agencies lack the capacity or motivation to effectively enforce, Congress should also consider granting individual consumers themselves the right to bring civil actions against companies for violating privacy regulations.

C. Privacy protections should also be enforced by state attorneys general

State attorneys general should also be empowered to enforce privacy. A single agency cannot hope to police the entire digital ecosystem. State attorneys general do a large volume of important work in this area, both enforcing privacy laws and providing valuable guidance to companies trying to comply with the law.

Attorneys general frequently provide companies with ongoing guidance to help businesses understand, adapt to, and comply with legal requirements

---

(Apr. 6, 2018), https://www.georgetowntech.org/news-fullposts/2018/4/7/april-6-2018-georgetowns-david-vladeck-outlines-challenges-opportunities-for-incoming-ftc-commissioners.

[29] The FTC has come under criticism for not doing enough to enforce its consent decrees. *See* Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation*, Techonomy, May 4, 2018, https://techonomy.com/2018/05/facebook-whatsapp-lesson-privacy-protection-necessary-innovation/. And the FCC has been widely criticized for not doing enough to protect security and privacy of phone users. *See* Craig Timberg, *How Spies Can Use Your Cellphone to Find You—and Eavesdrop on Your Calls and Texts, Too*, Wash. Post, May 30, 2018, https://www.washingtonpost.com/business/technology/how-spies-can-use-your-cellphone-to-find-you--and-eavesdrop-on-your-calls-and-texts-too/2018/05/30/246bb794-5ec2-11e8-a4a4-c070ef53f315_story.html; *Wyden Demands FCC Investigate Unauthorized Tracking of Americans' Cell Phones* (May 11, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-demands-fcc-investigate-unauthorized-location-tracking-of-americans-cell-phones; Violet Blue, *FCC Shrugs at Fake Cell Towers Around the White House*, Engadget, June 8, 2018, https://www.engadget.com/2018/06/08/fcc-shrugs-at-fake-cell-towers-around-the-white-house/.

and best practices. As explained by scholar Danielle Citron, who wrote about the importance of state attorneys general in developing privacy standards,

> Attorneys general establish task forces with business leaders, advocacy groups, and experts in the hopes that participants reach consensus on best practices. They reach out to companies with concerns about products and services. Staff provide advice to companies.[30]

The guidance provided by state attorneys general is vitally important. For example, in 2012 Vermont Attorney General William Sorrell partnered with a local university to offer free penetration tests to businesses to help them identify basic security vulnerabilities.[31] Speaking at an event the following year, Sorrell said it was important to his office to create a collaborative working relationship with companies. "If we find vulnerability, we tell the company," he said.[32] That program was later integrated into the services of the recently-established Vermont Agency of Digital Services.[33]

State attorneys general also generate best practice guides. According to Citron,

> In preparing guides, staff consult with stakeholders from a broad range of interests. . . . Stakeholder meetings can involve dozens of participants: the goal is to get as many perspectives as possible. AG offices educate stakeholders about best practices.[34]

If federal agencies are given the extra authority and resources they desperately need to do more privacy and data security work, they will be better able to address large privacy and data security cases, but will still be

---

[30] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 759 (2016).
[31] *See id.*
[32] Paul Shukovsky, *State Attorneys General Are Crucial Force in Enforcement of Data Breach Statutes*, Bloomberg Law: Privacy & Data Security, Oct. 7, 2013, https://www.bna.com/state-attorneys-general-n17179877665/.
[33] *See* Vermont Agency of Digital Services, *Security Services* http://dii.vermont.gov/infrastructure/security (last visited Oct. 7, 2018).
[34] Citron, *supra* note 30, at 760.

overwhelmed without the complementary consumer protection support of state attorneys general in thousands of small cases each year.[35]

To ensure that consumers receive the best protection they possibly can, state attorneys general must be given the ability to help enforce any new federal standard. This type of authority exists—and has been successful—under the Children's Online Privacy Protection Act.[36]

D. Protections for Americans' private information should be forward-looking and flexible

Any new legislation on privacy and/or data security must also be designed to be forward-looking and flexible, with built-in mechanisms to foster regulatory agility. We do not know what the next privacy or data security threat is going to be, but plainly there will be one, and it will arise faster than Congress will be able to react. Any broad privacy law must therefore include a mechanism for updating standards in accordance with shifting threats.

The need for regulatory agility is currently being met by state legislatures. In recent years, not only has California passed the California

---

[35] For example, according to the Massachusetts State Attorney General's Office, Massachusetts alone saw 2,314 data breaches reported in 2013, 97% of which involved fewer than 10,000 affected individuals. *Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Energy & Commerce Comm.* (2015) (statement of Sara Cable, Assistant Att'y Gen., Office of Mass. State Att'y Gen.). Each data breach affected, on average, 74 individuals. *Id.*

[36] The Children's Online Privacy Protection Act enables state attorneys general to bring actions on behalf of residents of their states against operators of online sites or services that they believe have violated children's privacy regulations. 15 U.S.C. §6504. State attorneys general use this authority; indeed, just weeks ago, the State Attorney General of New Mexico filed a suit against several companies for alleged children's privacy violations. *See AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data* (Sept. 12, 2018), https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Announces_Lawsuit_Against_Tech_Giants_Who_Illegally_Monitor_Child_Location__Personal_Data_1.pdf.

Consumer Privacy Act,[37] but Vermont passed the Data Broker Act,[38] and between 2015 and 2018 at least 23 different states—from all regions of the country—passed data security or breach notification legislation.[39]

Given the high level of legislative activity currently taking place at the state level on these issues, the most straightforward way to preserve regulatory flexibility in privacy and data security would be simply to leave state legislative authority intact. To do this, new federal legislation should establish a floor, not a ceiling for privacy—thus allowing states to continue to pass stronger laws on their own. States will no doubt continue to actively use this authority, as they are already doing.

As an additional measure to support regulatory agility, any agency or agencies that are to be tasked with protecting the privacy and security of consumers' information should be given rulemaking authority. Indeed, FTC commissioners have directly asked Congress for rulemaking authority.[40]

---

[37] California Consumer Privacy Act, https://www.caprivacy.org/ (last visited October 7, 2018).

[38] Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers*, TechCruch, May 27, 2018, https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/.

[39] Since 2015, data security or breach notification legislation has been enacted in Alabama, Arizona, California, Connecticut, Delaware, Florida, Illinois, Iowa, Maryland, Montana, Nebraska, New Hampshire, New Mexico, North Dakota, Oregon, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, and Wyoming. *See* Nat'l Conf. State Legislatures, *2015 Security Breach Legislation* (Dec. 31, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx; Nat'l Conf. State Legislatures, *2016 Security Breach Legislation* (Nov. 29, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx; Nat'l Conf. State Legislatures, *2017 Security Breach Legislation* (Dec. 29, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/2017-security-breach-legislation.aspx; Natl' Conf. State Legislatures, *2018 Security Breach Legislation*, http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx (last visited Oct. 7, 2018).

[40] Maureen K. Ohlhausen, FTC Commissioner, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf ("Legislation in both areas – data security and breach notification – should give the FTC . . . rulemaking authority under the Administrative Procedure

Rulemaking enables agencies to adjust regulations as technology changes, as the FTC did just a few years ago with the COPPA Rule.[41] As a starting point, the FTC should be given rulemaking authority over data security, data brokers, and consumer privacy.

E. Protections for Americans' private information should take into account the context in which information is shared

There is no one-size-fits-all approach for privacy. Rather, privacy standards often must be context-specific, carefully tailored based on the avoidability of the information sharing, the sensitivity of the information shared, and the expectations of consumers. As it considers establishing comprehensive baseline privacy standards, Congress should therefore not assume that existing privacy laws should simultaneously be eliminated. Many of those existing narrower privacy laws have already been appropriately tailored to establish heightened privacy standards under specific circumstances, in accordance with important contextual considerations relating to unavoidability and sensitivity.

First, heightened standards should apply when information sharing is unavoidable or less avoidable by consumers. This is consistent with several existing laws that protect consumer information in specific contexts in which sharing is unavoidable—such as the information shared by students in an

---

Act"); *Oversight of the Federal Trade Commission: Hearing Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce* (2018) (statement of Joseph J. Simons, Chairman, Fed. Trade Commission) (stating he "support[s] data security legislation that would give . . . the authority to issue implementing rules under the Administrative Procedure Act"); *id.* (statement of Rebecca Kelly Slaughter, Comm'r) (calling for APA rulemaking authority); *id.* (statement of Rohit Chopra, Comm'r) (also supporting rulemaking authority, stating, "the development of rules is a much more participatory process than individual enforcement actions and it also gives clear notice to the marketplace rather than being surprised, and I think it would be a good idea.").

[41] Federal Trade Commission, *FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information by Amending Children's Online Privacy Protection Rule* (Dec. 19, 2012), https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

educational context,[42] by consumers in a financial context,[43] by customers in a telecommunications context,[44] and by patients in a medical context.[45]

This is also consistent with the FTC's evaluation of potentially problematic data-related practices under its Section 5 authority to prohibit unfair practices. When considering whether a practice is unfair, the FTC asks not only whether the practice is harmful, but also whether the practice is one that consumers can avoid. In its policy statement on unfairness, the FTC explained,

> Normally we expect the marketplace to be self-correcting, and we rely on consumer choice—the ability of individual consumers to make their own private purchasing decisions without regulatory intervention—to govern the market. We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory. However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.[46]

Whether or not information sharing is avoidable by a consumer is often tied to the question of whether or not a service or transaction is essential. When a service is essential—such as with phone service—information sharing may be considered unavoidable because the consumer cannot reasonably decline the service altogether. This, too, helps explain why

---

[42] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[43] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).
[44] 47 U.S.C. § 222.
[45] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).
[46] FTC, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

heightened privacy protections apply in the educational,[47] financial,[48] telecommunications,[49] and medical contexts—all of these contexts involve essential services.[50]

Heightened standards also should apply in contexts in which the information shared or typically shared is sensitive. For example, the Children's Online Privacy Protection Act recognizes that information about children deserves heightened protection.[51] Other laws recognize the heightened sensitivity of health information[52] and financial information.[53] In the past, the question of sensitivity has often been the most important in considering how well the law should protect consumers' information. Data analysis techniques have advanced over time, however, and it is becoming clear that classically sensitive information can often be deduced from categories of information not traditionally thought of as sensitive. For example, as computer scientist Ed Felten explained in testimony before the Senate Judiciary Committee regarding telephone metadata, "Calling patterns can reveal when we are awake and asleep; our religion . . . our work habits and our social attitudes; the number of friends we have; and even our civil and political affiliations."[54] In 2016 the FTC found that television viewing history can be considered sensitive information,[55] and the Federal Communications Commission (FCC) found that web browsing history can be considered sensitive.[56] Indeed, patent applications filed by Google indicate

---

[47] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[48] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).
[49] 47 U.S.C. § 222.
[50] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).
[51] 15 U.S.C. §§ 6501–6506.
[52] *E.g.* Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (1996).
[53] *E.g.* Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338, (1999).
[54] *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing before the S. Comm. on the Judiciary,* 113th Cong. 8-10 (2013) (statement of Edward Felten, Prof. of Computer Science and Public Affairs, Princeton Univ.).
[55] Complaint at ¶ 32, *FTC v. Vizio*, Case No. 2:17-cv-00758, D.N.J. (filed Feb. 6, 2017), *available at* https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.
[56] Federal Communications Commission, *Fact Sheet: The FCC Adopts Order to Give Broadband Consumers Increased Choice over Their Personal*

that it is possible to estimate user demographics and location information based on browsing histories.[57]

F. Congress should not eliminate existing protections for Americans' information

Finally, as Congress considers establishing new privacy and data security protections for Americans' private information, it should not eliminate existing protections that already benefit Americans under state or other federal laws. Americans are asking for *more* protections for their private information, not less. This explains why consumers—on both sides of the aisle—were outraged when Congress voted last year to eliminate strong privacy regulations that had been passed by the FCC.[58] Some lawmakers argued that repeal of the FCC's rules was needed to foster development of a consistent approach to privacy across the Internet.[59] But as FTC Commissioner Terrell McSweeny noted, "If consistency were truly the goal, then we would likely increase protections for privacy, rather than unraveling them. That is the policy conversation we ought to be having—instead we are fighting a rear-guard action defending basic protections."[60]

Information, https://apps.fcc.gov/edocs_public/attachmatch/DOC-341938A1.pdf.

[57] *See* U.S. Patent Application No. 13/652,198, Publication No. 20130138506 (published May 30, 2013) (Google Inc., applicant) ("demographics data may include a user's age, gender, race, ethnicity, employment status, education level, income, mobility, familial status (e.g., married, single and never married, single and divorced, etc.), household size, hobbies, interests, location, religion, political leanings, or any other characteristic describing a user or a user's beliefs or interests."); U.S. Patent Application No. 14/316,569, Publication No. 20140310268 (published Oct. 16, 2014) (Google Inc., applicant).

[58] *See* Matthew Yglesias, *Republicans' Rollback of Broadband Privacy Is Hideously Unpopular*, Vox, Apr. 4, 2017, https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll.

[59] *See* Alex Byers, *House Votes to Revoke Broadband Privacy Rules*, Politico, Mar. 28, 2017, https://www.politico.com/story/2017/03/house-votes-to-revoke-broadband-privacy-rules-236607.

[60] Terrell McSweeny, Commissioner, Fed. Trade Comm'n, Remarks on *"The Future of Broadband Privacy and the Open Internet: Who Will Protect Consumers?"* (Apr. 17, 2014), at 4, https://www.ftc.gov/system/files/

Congress also should not eliminate existing and future consumer protections at the state level. As noted above, state laws play an important role in filling gaps that exist in federal legislation. For example, a number of states have expanded the scope of their data security and breach notification laws to extend protections to previously unregulated market sectors and private data—and consumers in those states are benefiting from those existing laws. For example, Connecticut's data security and breach notification statute covers entities operating at multiple nodes of the health care pipeline.[61] California adopted a data security statute—the Student Online Personal Information Protection Act (SOPIPA)—that is tailored to online educational platforms.[62] SOPIPA prompted twenty-one other states to adopt student data security laws modeled on California's example.[63] Minnesota adopted a law requiring Internet Service Providers (ISPs) to maintain the security and privacy of consumers' private information.[64] And Texas now requires any nonprofit athletic or sports association to protect sensitive personal information.[65]

Some states have also expanded the types of information that data holders are responsible for protecting from unauthorized access, or for notifying consumers of when breached. For example, ten states have expanded breach notification laws so that companies are now required to notify consumers of unauthorized access to their biometric data—unique measurements of a person's body that can be used to determine a person's

---

documents/public_statements/1210663/mcsweeny_-_new_americas_open_technology_institute_4-17-17.pdf.

[61] C.G.S.A. § 38a-999b(a)(2) ("health insurer, health care center or other entity licensed to do health insurance business in this state, pharmacy benefits manager . . . third-party administrator . . . that administers health benefits, and utilization review company.").

[62] West's Ann.Cal.Bus. & Prof.Code § 22584(d)(1) (schools must "[i]mplement and maintain reasonable security procedures and practices . . . and protect that information from unauthorized access, destruction, use, modification, or disclosure.").

[63] https://ikeepsafe.org/last-years-education-data-privacy-legislation-trends/

[64] M.S.A. § 325M.05 (must "take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information.").

[65] V.T.C.A., Bus. & C. § 521.052 ("implement and maintain reasonable procedures . . . to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.").

identity.[66] This important step recognizes that a biometric identifier such as a fingerprint or iris scan—unlike an alphanumeric password—cannot be changed after it has been compromised. A large number of states also now require companies to notify consumers about breaches of medical or health data—information that can be used in aid of medical identity theft, potentially resulting in fraudulent healthcare charges and even introduction of false information into one's medical record.[67]

And states are doing other important work on privacy as well. In addition to the California Consumer Privacy Act,[68] California also has a law requiring notification about breaches of information collected through an automated license plate recognition system.[69] Vermont has the Data Broker Act.[70] And Illinois has the Biometric Information Protection Act.[71]

To avoid doing harm to consumers benefiting from these existing consumer protections, any federal legislation on privacy or data security must preserve strong state standards.

4. Conclusion

I am grateful for the Committee's attention to these important issues, and for the opportunity to present this testimony. I look forward to your questions.

---

[66] States that have done this include Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, and Wyoming.
[67] *See* Joshua Cohen, *Medical Identity Theft—The Crime that Can Kill You*, MLMIC Dateline (Spring 2015), *available at* https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-SE_Spring15.pdf ("A patient receiving medical care fraudulently can lead to the real patient receiving the wrong blood type, prescription, or even being misdiagnosed at a later time."). Medical or health data is covered by breach notification laws in Alabama, Arkansas, California, Delaware, Florida, Illinois, Kentucky, Maryland, Montana, Nevada, North Dakota, Oregon, Puerto Rico, Nevada, Rhode Island, Texas, Virginia, and Wyoming.
[68] California Consumer Privacy Act, https://www.caprivacy.org/ (last visited October 7, 2018).
[69] West's Ann.Cal.Civ.Code § 1798.82(h)
[70] Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers*, TechCruch, May 27, 2018, https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/.
[71] 740 ILCS 14/1 *et seq.*