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

before the
United States House of Representatives Subcommittee on Consumer Protection and Commerce of the Committee on Energy and Commerce
Protecting Consumer Privacy in the Era of Big Data

February 26, 2019

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to testify about the imminent need for a foundational federal consumer 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 is committed to protecting privacy as a fundamental human and civil right and as a necessity for securing other rights such as access to justice, equal protection, and freedom of expression. CDT has offices in Washington, D.C., and Brussels, and has a diverse funding portfolio from foundation grants, corporate donations, and individual 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 data realm. While in the private practice of law, I counseled some of the internet's earliest commercial websites; I served as a corporate privacy leader at General Electric, Amazon, and DoubleClick; and was honored to serve 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

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

Department of Homeland Security under Secretary Tom Ridge, I was the first statutorily mandated CPO in the federal service.

In my testimony before the Senate Committee on Commerce, Science, and Transportation in October, I said that it was time to acknowledge the impacts of ubiquitous data collection and sharing, and to pass clear rules that would provide certainty to both companies and consumers.[2] In the months since that hearing, the urgency for Congress to pass strong and comprehensive privacy protections has mounted. New investigative reporting has revealed an unbounded secondary market for Americans' sensitive information, such as location[3] and health data.[4] Data brokers continue to build secretive and detailed profiles that can be used to exploit or discriminate based on race, religion, gender, age, and other protected categories.[5] Consumers have made it clear that they want certainty, not surprises, when they entrust their personal information to a company. It's time for Congress to deliver the privacy protections we have been waiting for.

CDT's vision for our digital future is one in which technology supports human rights and human dignity. This future cannot be realized if people are forced to choose between protecting their personal information and using the technologies and services that enhance our lives. This future depends on clear and meaningful rules governing data processing; rules that do not simply provide people with notices and check boxes but actually protect them from privacy and security abuses and data-driven discrimination; protections that cannot be signed away.

We understand that drafting comprehensive privacy legislation is a complex endeavor. Over the past year we have worked with partners in civil society, academia, and various industry sectors to produce draft legislation that is both meaningful and workable. This testimony will discuss the components of our draft and why they should be incorporated into a federal privacy law.

---

[2] Statement of Nuala O'Connor, President & CEO, Ctr. for Democracy & Tech., before S. Comm. Commerce, Science & Transportation (Oct. 10, 2018), https://cdt.org/insight/nuala-oconnors-written-testimony-before-senate-commerces-consumer-data-privacy-hearing/.

[3] *See* Jennifer Valentino DeVries et al., *Your apps know where you were last night, and they're not keeping it a secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[4] Derek Kravitz & Marshall Allen, *Your medical devices are not keeping your health data to themselves*, Pro Publica (Nov. 21, 2018), https://www.propublica.org/article/your-medical-devices-are-not-keeping-your-health-data-to-themselves.

[5] Yael Grauer, *Here's a long list of data broker sites and how to opt-out of them*, Motherboard (March 27, 2018), https://motherboard.vice.com/en_us/article/ne9b3z/how-to-get-off-data-broker-and-people-search-sites-pipl-spokeo.

Privacy legislation must (1) provide individual rights to access, correct, delete, and port personal information; (2) require reasonable data security and corporate responsibility; (3) prohibit unfair data practices, particularly the repurposing or secondary use of sensitive data, with carefully scoped exceptions; (4) prevent data-driven discrimination and civil rights abuses; and (5) provide robust and rigorous enforcement, including additional personnel and original fining authority for the Federal Trade Commission (FTC). The future of this country's technology leadership depends on this Congress passing clear, comprehensive rules of the road that facilitate trust between consumers and the organizations that collect and use their data.

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:

- A New York Times investigation found that many of the apps that collect location information for localized news, weather, and other location services repurpose or share that information with third parties for advertising and other purposes. The investigation also suggested that users believe they are sharing location data for a specific location-based service, not giving free rein for any use sharing.[6]

[6] DeVries, *supra* note 3.

- A Congressional investigation found that location data sold to third parties by internet service providers (ISPs) was used by prison officials to track innocent Americans.[7] A Motherboard investigation found that bounty hunters could also access detailed location data sold by ISPs.[8]
- General Motors bragged in September that the company had secretly gathered data on driver's radio-listening habits and where they were when listening "just because [they] could."[9] This data was exfiltrated from cars using built-in WiFi, which consumers can only use if they agree to GM's terms of service.
- 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.[10]
- Application developer Alphonso created over 200 games, including ones targeted at children, that turn on a phone's microphone solely for marketing purposes.[11]
- Facebook permitted housing advertisements to be obscured from parents, disabled people, and other groups protected by civil rights laws.[12]

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 developed a "common law" of privacy and security through its enforcement actions.[13] Creating proactive privacy rights through an episodic approach will not be able to keep up with advances in technology and the explosion of device and app manufacturers.

Moving Beyond Notice and Consent

[7] *See* ltr from Sen. Ron Wyden to Randall L. Stephenson, President and CEO, AT&T (May 8, 2018), https://www.documentcloud.org/documents/4457319-Wyden-Securus-Location-Tracking-Letter-to-AT-amp-T.html.
[8] Joseph Cox, *I gave a bounty hunter $300. Then he located our phone*, Motherboard (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.
[9] Cory Doctorow, Every minute for three months, GM secretly gathered data on 90,000 drivers' radio-listening habits and locations, BoingBoing (Oct. 23, 2018), https://boingboing.net/2018/10/23/dont-touch-that-dial.html.
[10] Kevin Draper, Madison Square Garden Has Used Face-Scanning Technology on Customers, NYT, Mar. 13, 2018.
[11] 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.
[12] 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.
[13] Daniel Solove and Woody Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia L. Rev. 583, (2014).

Existing privacy regimes rely too heavily on the concept of notice and consent, placing an untenable burden on consumers and failing to rein in harmful data practices.[14] These frameworks simply require companies to provide notice of their data practices and get some kind of consent—whether implied or express—or provide users with an array of options and settings. This model encourages companies to write permissive privacy policies and entice users to agree to data collection and use by checking (or not unchecking) a box.

This status quo burdens individuals with navigating every notice, data policy, and setting, trying to make informed choices that align with their personal privacy interests. The sheer number of privacy policies, notices, and settings or opt-outs one would have to navigate is far beyond 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.[15] Further, people operate under woefully incorrect assumptions about how their privacy is protected.[16] Privacy self-management alone is neither scalable nor practical for the individual. Burdening individuals with more and more granular decisions, absent some reasonable boundaries, will not provide the systemic changes we need.[17]

Moreover, people can be harmed by data processors with whom they have no direct relationship, making control impossible. Last year, 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.[18] 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.

---

[14] 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).

[15] Grauer, *supra* note 5.

[16] 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.

[17] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013); Aleecia McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: A Journal of Law and Policy 543, (2008); Joel Reidenberg, Presentation, Putting Disclosures to the Test (2016), available at https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test.

[18] 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/.

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.[19] 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.[20]

Another weakness of notice-and-choice models is their inability to address discriminatory uses of data. Commercial data can be used in ways that systematically discriminate based on minority or protected classes such as race, age, gender, sexual orientation, disability, or economic status. Data-driven discrimination is inherently difficult for individuals to detect and avoid, and cannot be solved with a check box.

CDT is not the only entity to critique notice and consent as the predominant privacy control in U.S. law. 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."[21] 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 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 pass explicit and targeted privacy protections for consumer data. As discussed below, legislation should (1) provide individual rights to access, correct, delete, and port personal information; (2) require reasonable data security and corporate responsibility; (3) prohibit unfair data practices, particularly the repurposing or secondary use of sensitive data,

---

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

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

[21] 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.

with carefully scoped exceptions; (4) prevent data-driven discrimination and civil rights abuses; and (5) provide a robust and fair enforcement mechanism including original fining authority for the FTC.[22]

Individual Rights in Data

A federal law must include basic rights for individuals to access, correct, delete, and port their personal data.[23] CDT's draft legislation would provide broad access and deletion rights, with tailored exceptions to account for technical feasibility, legitimate needs such as fraud detection and public interest research, and free expression rights. It also provides a right to dispute the accuracy and completion of information used to make critical decisions about a person, such as eligibility for credit, insurance, housing, employment, or educational opportunities. No one should be subject to life-altering decisions based on inaccurate or incomplete data. The draft also includes a right to transfer one's data from one service to another, where technically feasible (known as "data portability").

These rights would apply not only to information directly disclosed to a covered entity but also to information inferred by the covered entity, since inferences can often be more sensitive and opaque to users (e.g., inferring a medical condition based on someone's non-medical purchase history). A 2013 report from the Senate Commerce Committee found that data brokers created and sold consumer profiles identifying people as "Rural and Barely Making It," "Ethnic Second-City Strugglers," and "Retiring on Empty: Singles."[24] This information can be used to target vulnerable consumers with potentially harmful offers, such as payday loans.[25]

A federal law must also enshrine the right to know how and with whom personal data is shared. Our draft requires disclosure of the names of third parties with whom information is shared. Some models only require disclosure of the categories of entities with whom data is

---

[22] 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.
[23] Rob Pegoraro, *Web companies should make it easier to make your data portable: FTC's McSweeny*, USA Today (Nov. 12, 2017), https://eu.usatoday.com/story/tech/columnist/2017/11/12/web-companies-should-make-easier-make-your-data-portable-ftcs-mcsweeny/856814001/.
[24] Staff Report, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, S. Committee on Commerce, Science & Transportation (Dec. 18, 2013), https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.
[25] *See, e.g.*, Upturn, Led Astray: Online Lead Generation and Payday Loans (Oct. 2015), https://www.upturn.org/static/reports/2015/led-astray/files/Upturn_-_Led_Astray_v.1.01.pdf.

shared, which tells consumers and regulators very little about where the data is going and how it's being used.

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 California Consumer Privacy Act. They have been recognized by the U.S. government and international bodies for decades, albeit in voluntary form.[26] 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.

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.

Affirmative Obligations to Protect Data

Entities that collect, use, and share data have a responsibility to safeguard it and prevent misuse. CDT's draft legislation would require covered entities to adopt reasonable data security practices and engage in reasonable oversight of third parties with whom they share personal information. These obligations recognize the reality that participating in modern society often means ceding control of one's personal information. The entities we trust with our data should handle it with care.

Our draft would also require covered entities to publish detailed disclosures of their data practices in a standardized, machine readable format that can be scrutinized by regulators and advocates. This annual report would be in addition to the real time disclosures made to users at the time they sign up for a new service or activate a device, or the privacy policies that operate at any one time. Ideally, these reports will result in detailed and standardized accounts of data processing that can be used by regulators, advocates, and privacy researchers to scrutinize covered entities on behalf of consumers.

Like individual rights, data security and standardized notices should be relatively non-controversial, but they are not enough to protect privacy. Proposals that include only access/correction/deletion rights and transparency, without meaningful limits on the collection and use of data, are insufficient.

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

Prohibiting Unfair Data Practices

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. CDT's draft would prohibit the following data processing practices, with some exceptions, when the processing is not required to provide or add to the functionality of a service or feature that the user has affirmatively requested:

- The processing of biometric information to identify a person;
- The processing of precise geolocation information;
- The processing of health information;
- The use of children's information for targeted advertising and disclosure to third parties;
- The licensing or sale to third parties of the contents of communications or the parties to a communication (such as call or email logs);
- The retention, use, or disclosure of audio and visual recordings; and
- The use of probabilistic inferences to tracking people across different devices.

These categories involve information that is particularly sensitive and types of processing or repurposing that are typically unexpected and difficult to foresee. If a user downloads a mapping service and agrees to provide precise location information, that information should only be used to provide and improve the performance of that service and not, for example, to provide data to retailers about the user's proximity to their stores. These guardrails would provide certainty to companies while allowing them to provide valuable data-driven services, and would allow users to share sensitive data with reasonable expectations that it will be safeguarded. Technology changes quickly and it can be difficult for the law to keep pace, so we have also drafted a safety valve whereby companies can petition the FTC to create specific exceptions to these prohibitions. Our bill also includes narrowly scoped exceptions for data security and fraud prevention and emergencies.

Preventing data-driven discrimination

In its 2016 Big Data report, the Federal Trade Commission (FTC) found that "big data offers companies the opportunity to facilitate inclusion or exclusion." Unchecked data processing and algorithmic decisionmaking can amplify discrimination based on race, gender, sexual orientation, ability, age, financial status, and other group membership. Since the FTC's report, discriminatory data practices have continued, but little has been done to address them. CDT and 42 other organizations wrote in a letter to Congress that any federal privacy legislation must address data-driven discrimination.[27] The letter states:

> Civil rights protections have existed in brick-and-mortar commerce for decades. It is time to ensure they apply to the internet economy as well. Platforms and other online services should not be permitted to use consumer data to discriminate against protected classes or deny them opportunities in commerce, housing, and employment, or full participation in our democracy.[28]

The data economy offers new opportunities to target information and personalize experiences, but it also creates new opportunities for exclusion based on protected group membership and for exploitative targeting.

- Journalists and researchers have demonstrated how advertising platforms can be used to target housing, job, and credit ads away from protected classes (e.g., excluding categories like "mothers" or "wheelchair users" from seeing a housing ad). Targeting affects who gets to learn about and apply for an opportunity.[29]

---

[27] Ltr from 43 organizations to members of Congress, Address data-driven discrimination, protect civil rights (Feb. 13, 2019), http://civilrightsdocs.info/pdf/policy/letters/2019/Roundtable-Letter-on-CRBig-Data-Privacy.pdf.

[28] *Id.*

[29] *See* Till Speicher et al., Potential for Discrimination in Online Targeted Advertising, Proceedings of Machine Learning Research 81:1–15, 8, T. 2 (2018), http://proceedings.mlr.press/v81/speicher18a/speicher18a.pdf; Julia Angwin and Terry Parris Jr., Facebook Lets Advertisers Exclude Users by Race, ProPublica (Oct. 28, 2016),https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race; Julia Angwin, Ariana Tobin & Madeleine Varner, Facebook (Still) Letting Housing Advertisers Exclude Users by Race,ProPublica (Nov. 21, 2017),https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin; Amit Datta, Michael Carl Tschantz & Anupam Datta, Automated Experiments on Ad Privacy Settings: A Tale of Opacity,Choice, and Discrimination, In Proceedings on Privacy Enhancing Technologies (2015), https://arxiv.org/abs/1408.6491; Amit Datta et al., Discrimination in Online Advertising: A Multidisciplinary Inquiry, in Proceedings of Machine Learning Research 81:1–15, 3–7 (2018), http://proceedings.mlr.press/v81/datta18a/datta18a.pdf; Julia Angwin, et. al, Dozens of Companies are

- Employers often rely on services that proactively match them with job candidates, but if those algorithms are based on past hiring preferences, they can replicate discriminatory patterns.[30]
- Predictive analytics used to target health interventions or set insurance rates may be less accurate for minority groups that have historically been excluded from research data.[31]
- Advertisers have leveraged data to target risky, undesirable, or even fraudulent opportunities based on sensitive characteristics.[32] The data broker industry has aggregated information from disparate sources and used it to create marketing segments such as "urban scramble," "diabetes interest," and sexual assault survivors.[33]
- The payday loan and for-profit college industries have used sensitive segments as well as deceptive data collection interfaces to generate leads.[34]

CDT's draft legislation would direct the FTC to promulgate rules addressing unfair advertising practices, particularly those that result in unlawful discrimination in violation of civil rights law.

Meaningful enforcement mechanisms

Affirmative individual rights and data collection and use restrictions may ultimately be meaningless absent strong enforcement. While we believe that the FTC has been effective as the country's "top privacy cop," it is also an agency that desperately needs more resources.

Using Facebook to Exclude Older Workers From Jobs, Dec. 20, 2017, https://www.propublica.org/article/facebook-ads-age-discrimination-targeting.

[30] Miranda Bogen & Aaron Rieke, Help Wanted: An Examination of Hiring Algorithms, Equity, & Bias (Dec. 2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

[31] *See* Kadija Ferryman & Mikaela Pitcan, Fairness in Precision Medicine (Feb. 2018), https://datasociety.net/wp-content/uploads/2018/02/Data.Society.Fairness.In_.Precision.Medicine.Feb2018.FINAL-2.26.18.pdf; Center for Democracy & Technology, Healgorithms: Understanding the Potential for Bias in mHealth Apps (Sept. 13, 2018), https://cdt.org/insight/healgorithms-understanding-the-potential-for-bias-in-mhealth-apps/.

[32] *See, e.g.*, Upturn, *supra* note 25.

[33] Fed. Trade Comm'n, Data Brokers: A Call for Transparency & Accountability at v (May 2014),https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; Pam Dixon, Statement before the Senate Committee on Commerce, Science and Transportation, Hearing on What Information Do Data Brokers Have on Consumers, and How Do They Use It? At 9, 12–13 (Dec. 18, 2013),https://www.commerce.senate.gov/public/_cache/files/e290bd4e-66e4-42ad-94c5-fcd4f9987781/BF22BC3239AE8F1E971B5FB40FFEA8DD.dixon-testimony.pdf.

[34] Upturn, *supra* note 25.

Funding for the agency has fallen five percent since 2010, and its resources are strained.[35] In 2015, the FTC had only 57 full-time staff working in the Division of Privacy and Identity Protection, with additional staff working in enforcement and other areas that could touch on privacy.[36] 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.[37] 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.

Relying solely on consent-decree enforcement is 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 terms of its consent order in 2012, this was approximately five hours' worth of Google's revenue at the time.[38]

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.[39] Employing their expertise will be necessary for a new federal privacy law to work. A law with the scope CDT 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.

---

[35] 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.

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

[37] 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.

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

[39] 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.

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 comprehensive privacy 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 its leadership and pass a comprehensive privacy law for this country.