Statement of Michelle Richardson, Director, Privacy & Data
Center for Democracy & Technology

before the
United States Senate Committee on the Judiciary
GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation

March 12, 2019

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to testify about the importance of crafting a federal consumer privacy law that provides meaningful protections for Americans and clarity for entities of all sizes and sectors. 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]

The United States should be leading the way in protecting digital civil rights. This hearing is an opportunity to learn how Congress can improve upon the privacy frameworks offered in the European Union via the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) to craft a comprehensive privacy law that works for the U.S. Our digital future should be 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

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

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.

Congress should resist the narratives that innovative technologies and strong privacy protections are fundamentally at odds, and that a privacy law would necessarily cement the market dominance of a few large companies. Clear and focused privacy rules can help companies of all sizes gain certainty with respect to appropriate and inappropriate uses of data. Clear rules will also empower engineers and product managers to design for privacy on the front end, rather than having to wait for a public privacy scandal to force the rollback of a product or data practice.

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.

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 Comprehensive 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.[2] The secondary use and sharing of location data creates a serious safety risk, particularly for survivors of intimate partner violence, sexual assault, and gender-based violence. The National Network to End Domestic Violence (NNEDV) advises survivors who are concerned they may be tracked to consider leaving their phones behind when traveling to sensitive locations or turning their phones off altogether.[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.[4] A Motherboard investigation found that bounty hunters could also access detailed location data sold by ISPs.[5]
- 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."[6] This data was exfiltrated from cars using built-in WiFi, which consumers can only use if they agree to GM's terms of service.

---

[2] DeVries, *supra* note 3.
[3] *See* Technology Safety, Data Privacy Day 2019: Location Data & Survivor Safety (Jan. 28, 2019), https://www.techsafety.org/blog/2019/1/30/data-privacy-day-2019-location-data-amp-survivor-safety.
[4] *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.
[5] 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.
[6] 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.

- 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.[7]
- Application developer Alphonso created over 200 games, including ones targeted at children, that turn on a phone's microphone solely for marketing purposes.[8]
- Facebook permitted housing advertisements to be obscured from parents, disabled people, and other groups protected by civil rights laws.[9]

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.[10] 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.

Protecting Americans' Digital Civil Rights while Providing Clarity for Industry

This hearing has been framed through the lens of the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These two legal regimes, which dominated privacy headlines in May and June of last year, have established both a foundation and a point of comparison for any federal privacy framework. However, we should recognize that it remains early days for both laws. The CCPA does not go into effect until next year, and both legislative and regulatory tweaks to the law are likely. There is more to be said about the GDPR, though serious enforcement activities only began in January of 2019.

I. GDPR Operationalizes Long-standing Privacy Principles Broadly Recognized Here and Abroad

The concern that privacy laws can disproportionately burden small businesses and start-ups is well-intentioned, but it is ultimately a false choice to pit strong privacy laws against

[7] Kevin Draper, Madison Square Garden Has Used Face-Scanning Technology on Customers, NYT, Mar. 13, 2018.
[8] 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.
[9] 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.
[10] Daniel Solove and Woody Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia L. Rev. 583, (2014).

innovation and economic interests.[11] The reality is that strong privacy laws, that establish clear ground rules can create a level playing field for businesses large and small, and protect consumers from unfair, surprising, and privacy-invading practices.

At its core, the GDPR embraces six key principles for processing information, including transparency, purpose limitations, and the integrity and confidentiality of information.[12] None of these principles are new. Rather, they reflect a European formulation of longstanding Fair Information Practice Principles, **which originated in the United States** and are at the core of our own privacy rules, including the federal Privacy Act.[13] These principles are buttressed by a set of individual rights to data, which include rights to be informed, access, correct, and delete information.[14]

These rights were not newly created for the GDPR and many were previously core components of the prior EU Data Protection Directive, which went into effect in 1995. It is also important to acknowledge that, under the GDPR, none of these rights are absolute.[15] They have to weighed against rights to free expression and legitimate business needs. As this committee considers what the shape of U.S. federal privacy law could look like, the United States can — and should — debate the scope and contours of these GDPR rights and principles, but we should not consider them to be utterly foreign, either in terms of individual privacy protections or businesses' responsibilities to consumers.

The challenge is that while the GDPR may have clear overarching goals, it does not include explicit recommendations or specific prohibitions in a way that is immediately clear for companies.[16] Instead, the GDPR established a complicated legal regime, consisting of 99 different articles and 173 explanatory recitals. This structure may create costs for businesses, but before critics jump to the assumption that the GDPR has unfairly burdened small- and medium-sized businesses, we must ask what sorts of business models the critics are speaking about.

---

[11] See Noah Joshua Philips, Commissioner, Fed. Trade Comm'n, Prepared Remarks at the Internet Governance Forum USA, "Keep It: Maintaining Competition in the Privacy Debate" (July 27, 2018).
[12] GDPR Article 5.
[13] Robert Gellman, Fair Information Practices: A Basic History (Apr. 10, 2017), available at https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.
[14] For a summary, see "Individual Rights" from the UK Information Commissioner's Office, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.
[15] GDPR Recital 4.
[16] Andrew Burt, Why Privacy Regulations Don't Always Do What They're Meant To, Harvard Business Review (Oct. 23, 2018), https://hbr.org/2018/10/why-privacy-regulations-dont-always-do-what-theyre-meant-to.

II. There is No Overarching Data on the Impact of GDPR

The evidence that GDPR has hurt small- and medium-sized businesses is, at best, anecdotal and ultimately inconclusive. Small businesses are the backbone of the European economy -- SMEs in the EU28 account for 99.8% of the total number of enterprises and 66.6% of total EU employment.[17]

There is no evidence that GDPR has shut down these businesses. While GDPR enforcement has only recently begun, it appears to have mainly created a shift in the context of data sales and online advertising; something that was at the center of the Cambridge Analytica scandal. It is true that the GDPR has brought new challenges for data brokers, credit reporting agencies, and advertising companies,but this is not a surprising list of companies.[18] As the UK Information Commissioner has explained, there is "a dynamic tension" between the way these businesses operate and the underlying principles of the GDPR.[19] Rather than blame the complexity of GDPR, we might also reflect on the complexity of online advertising and data brokerage.

These companies collect, share and sell personal information, even though consumers have no real relationship with them.[20] Despite growing public concern about their practices, data brokers have resisted even measured and modest calls for regulation.[21] Trade associations called unconstitutional a recent law passed in Vermont that simply requires these companies to join a public registry and provide more transparency into their practices. The companies most impacted by GDPR are those that lack transparency and basic accountability to individuals. This includes the ecosystem that facilitates third-party online behavioral advertising, but rather than blame privacy rules, we ought to acknowledge the longstanding transparency and accountability issues within online advertising, and the resulting impact that has across the internet.

Much has been made of the fact that more than 1,000 U.S. news sites shut down service to European users after May 25, but we should first acknowledge that most of these sites and

---

[17] PwC, Innovation and Digital Transformation: How do European SMEs perform? (Oct. 2018), available at https://www.pwc.nl/nl/assets/documents/pwc-europe-monitor-innovation-sme.pdf.
[18] Amit Katwala, Forget Facebook, mysterious data brokers are facing GDPR trouble, Wired UK (Nov. 8, 2018), https://www.wired.co.uk/article/gdpr-acxiom-experian-privacy-international-data-brokers.
[19] Aliya Ram & Madhumita Murgia, Data brokers: regulators try to rein in the 'privacy deathstars', FT (Jan. 7, 2019), https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521.
[20] Joseph Jerome, Where Are the Data Brokers?, Slate Future Tense (Sept. 25, 2018), https://slate.com/technology/2018/09/data-brokers-senate-hearing-privacy.html.
[21] Sam Pfeifle, Industry Reaction to FTC Data Brokers Report: Eh., IAPP (May 28, 2014), https://iapp.org/news/a/industry-reaction-to-ftc-data-brokers-report-eh/.

services are owned by a few companies that had small amounts of traffic in the European Union.[22] These decisions were portrayed as part of a "last minute" scramble to figure out how to comply with the GDPR, but companies had two full years to prepare for the GDPR. Online advertisers were only just rolling out new transparency and consent frameworks weeks before last May.

USA Today provides a perfect counter example. Rather than block European readers, USA Today simply removed some ad-related software that surreptitiously harvests information and tracks the online behaviors of its readers. This is the complexity of adtech: USA Today's American website is 5.5 megabytes in size and includes more than 800 ad-related requests for information involving 188 different domains. In contrast, the EU-facing site is less than half a megabyte in size and contains no third-party content. This website not only does less surreptitious tracking, but it also benefits from loading faster.[23]

Other publishers have taken more creative approaches. After the GDPR went into effect, The New York Times cut off advertising exchanges in Europe — companies neither you nor I have ever heard of — and kept growing ad revenue for itself.[24] The paper's Vice President of Advertising Data last week called privacy laws that reduce reliance on third-party ad targeting a "win-win-win" for publishers, advertisers, and importantly, consumers.[25] Last Friday, the Washington Post committed to "go beyond cookie-based ad targeting and match ads to people without being 'creepy'."[26] The Local Media Consortium currently is exploring consumer-friendly privacy policies and standards for smaller online publishers.[27]

It is important to note that not every withdrawal from the market is a loss for consumers. Klout, for example, was a marketing company that peddled "Klout" scores, which

---

[22] Tronc owns companies such as the Los Angeles Times, Chicago Tribune, New York Daily News, Orlando Sentinel, Baltimore Sun, etc. and Lee Enterprises owns 46 newspapers across 21 states. GDPR: US News Sites Unavailable to EU Users Under New Rules (May 25, 2018), https://www.bbc.com/news/world-europe-44248448.

[23] Mathew Ingram, Four days into GDPR, US publishers are starting to feel the effects, Columbia Journalism Review (May 29, 2018), https://www.cjr.org/the_new_gatekeepers/gdpr-rules-publishers.php.

[24] Jessica Davies, After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue, Digiday (Jan. 16, 2019), https://digiday.com/media/new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/.

[25] Kendell Timmers, VP of Advertising Data, N.Y. Times, Third-Party Data Is A Bad Habit We Need To Kick, AdExchanger (Feb. 22, 2019), https://adexchanger.com/the-sell-sider/third-party-data-is-a-bad-habit-we-need-to-kick/.

[26] Lucia Moses, The Washington Post is trying to go beyond cookie-based ad targeting and match ads to people without being 'creepy' (Mar. 8, 2019), https://www.businessinsider.com/washington-post-goes-beyond-cookie-based-ad-targeting-with-feedbuilder-2019-3.

[27] https://infotrust.org/multi-stakeholder-convening-process-to-develop-consumer-friendly-privacy-policies-and-standards/

were an attempt to quantify online influence.[28] The system encouraged linking multiple accounts, which could help increase one's score.[29] Despite the fact that most people did not know they had a Klout score, they were used to punish and reward people in real life, including in decisions about hiring and customer service (one hotel used them to determine which guests' got a free room upgrade).[30] The scores themselves were ripe to be gamed, abused, and ultimately mocked.[31] The company relied on easy access to information from Facebook, Instagram, Twitter, and other platforms, but there is ample evidence that Klout's proprietary black box algorithm didn't work and did not actually serve advertisers.[32] Klout ceased to be relevant years ago, and the GDPR provided a convenient excuse, in the words of the company, to "expediate[] our plans to sunset Klout."[33] The GDPR was ultimately just the final nail in the service's coffin.

Rather than see this as a problem with the GDPR, we should be asking what rights ought to be attached to services that score us based off our data in ways that have real-world impacts. Online scoring is rampant and too often unregulated. Klout shut down before it had to reveal exactly what data it held about its users and how it was being processed.

Focusing on companies whose business models and privacy-invasive offerings made GDPR compliance challenging also ignores the very real consumer benefits that have been derived as a result of the Regulation. As part of GDPR compliance, companies have been investing in new data security systems to protect data and ensure it is only accessed by appropriate staff.[34] GDPR has been an opportunity for all organizations to engage in a sort of "spring cleaning" to look at the data they were holding, why they held it, and whether it was accurate.[35] According to a survey from Cisco:

---

[28]Seth Stevenson, What Your Klout Score Really Means, Wired (Apr. 24, 2012), https://www.wired.com/2012/04/ff-klout/.
[29] Id.
[30] Id.
[31] Will Oremus, Klout Is Shutting Down Just In Time to Not Reveal How Much It Knew About Us, Slate (May 10, 2018), https://slate.com/technology/2018/05/klout-is-dead-just-in-time-of-europes-gdpr-privacy-law-thats-not-a-coincidence.html.
[32] Garett Sloane, Out of Klout: The Social Media Scoring Service in Shutting Down, AdAge (May 10, 2018), https://adage.com/article/digital/klout-social-media-scoring-service-shutting/313470/.
[33] Will Oremus, Klout Is Shutting Down Just In Time to Not Reveal How Much It Knew About Us, Slate (May 10, 2018), https://slate.com/technology/2018/05/klout-is-dead-just-in-time-of-europes-gdpr-privacy-law-thats-not-a-coincidence.html.
[34] Steve Ranger, GDPR proves that tech giants can be tamed, ZDNet (May 24, 2018), https://www.zdnet.com/article/gdpr-is-already-a-success-whether-you-like-it-or-not/.
[35] Zara Rahman, Here We Are, With the GDPR, Engine Room (Apr. 24, 2018), https://www.theengineroom.org/here-we-are-with-the-gdpr/.

> The findings from this study provide strong evidence that organizations are benefitting from their privacy investments beyond compliance. Organizations that are ready for GDPR are experiencing shorter delays in their sales cycle related to customers' data privacy concerns than those that are not ready for GDPR. GDPR-ready organizations have also experienced fewer data breaches, and when breaches have occurred, fewer records were impacted, and system downtime was shorter. As a result, the total cost of data breaches was less than what organizations not ready for GDPR experienced.
>
> Even though companies have focused their efforts on meeting privacy regulations and requirements, nearly all companies say they are receiving other business benefits from these investments beyond compliance. These privacy-related benefits are providing competitive advantages to organizations.[36]

Whatever the complexity of the GDPR, Cisco also found that the two biggest challenges for companies under the GDPR were data security requirements and employee training.[37] Data security requirements and employee training are basic and foundational privacy practices; the fact that these requirements have proven challenging is, itself, evidence of how cavalier companies have been with respect to data privacy.

III. Early GDPR Enforcement

A survey of early GDPR enforcement activities shows that European Data Protection Authorities (DPAs) have focused on certain sensitive data types, including geolocation and health data, and failures by companies to adequately inform individuals of their data practices. While large companies have been subject to the most scrutiny, regulators have signaled a willingness to work with smaller companies.[38]

A. Regulators have worked with smaller businesses towards GDPR compliance

For example, the French Commission nationale de l'informatique et des libertés (CNIL) issued a warning against small advertising technology company Vectuary for failing to collect

---

[36] Howard Solomon, Privacy worries delaying sales, says Cisco study, but don't blame GDPR, ITWorld Canada (Feb. 1, 2019), https://www.itworldcanada.com/article/privacy-worries-delaying-sales-says-cisco-study-but-dont-blame-gdpr/414712.

[37] Cisco, Data Privacy Benchmark Study (Jan. 2019), available at https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf.

[38] E.g., UK Information Commissioner's Office, Blog: Adtech fact finding forum shows consensus on need for change (Mar. 2019), https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-fact-finding-forum-shows-consensus-on-need-for-change/%E2%80%AC.

appropriate consent for obtaining geolocation data from an scripts embedded in the mobile applications of its partners.[39] While some argued this could be the end of online advertising as we know it,[40] the probe was recently dropped after the company made changes to its disclosures.[41] The CNIL also worked with several other location analytics companies.[42] As the CNIL has explained, data protection regulators are not interested in "fin[ing] companies out of existence if there is any alternative" and "will be more gentle and take the time to first explain to companies how they have to do things."[43]

Some of the early fines under the GDPR reflect this. They are proportional and targeted at serious privacy breaches. In December, a Portuguese hospital was fined €400,000 after it was found that the hospital lacked controls around access to patient data. For example, 985 hospital employees had access rights of a medical doctor, even though only 296 doctors were on staff,[44] and doctors were granted unrestricted access to patient files regardless of their role.[45] A German social media and chat service received a €20,000 fine for storing social media passwords in plain text.[46] A local business in Austria was also fined €4,800 in October last year for unlawful surveillance of a public space.[47]

B. Regulators have specifically focused on the activities of Facebook and Google

In contrast to the approach taken with smaller entities, regulators have trained their sights on the largest data-driven technology companies. Ireland, which is where many American technology companies are based for their EU operations, is a good example of this. The Irish

---

[39] CNIL, Mobile applications: formal notice for failure to consent to geolocation data processing for advertising targeting purposes (Nov. 9, 2018), https://www.cnil.fr/fr/applications-mobiles-mise-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire-2. .
[40] Natasha Lomas, How a Small French Privacy Ruling Could Remake Adtech for Good (Nov. 20, 2018), https://techcrunch.com/2018/11/20/how-a-small-french-privacy-ruling-could-remake-adtech-for-good/.
[41] Rebecca Hill, French data watchdog withdraws probe from location data guzzling adtech biz Vectaury, The Register (Feb. 27, 2019), https://www.theregister.co.uk/2019/02/27/cnil_gdpr_vectaury/.
[42] Greg Sterling, Data location vendor worked with GDPR regulator on data consent model, yielding 70% opt-in rates, Martech Today (Feb. 11, 2019), https://martechtoday.com/data-location-vendor-worked-with-gdpr-regulator-on-data-consent-model-yielding-70-opt-in-rates-230653.
[43] Alliston Schiff, GDPR Will Pick Up Momentum In 2019, AdExchanger (Jan. 2, 2019), https://adexchanger.com/privacy/gdpr-will-pick-up-momentum-in-2019/.
[44] Matt Kelly, First GDPR Enforcement Action Didn't Even Involve a Data Breach (Dec. 5, 2018), https://www.jdsupra.com/legalnews/first-gdpr-enforcement-action-didn-t-11429/.
[45] Anna Oberschelp de Meneses & Kristof Van Quathem, Portuguese hospital receives and contests 400,000 € fine for GDPR infringement, Covington Inside Privacy (Oct. 26, 2018), https://www.insideprivacy.com/data-privacy/portuguese-hospital-receives-and-contests-400000-e-fine-for-gdpr-infringement/.
[46] Tomáš Foltýn, German chat site faces fine under GDPR after data breach, WeLiveSecurity (Nov. 27, 2018), https://www.welivesecurity.com/2018/11/27/german-chat-site-faces-fine-gdpr/.
[47] Lukas Feiler, Takeaways from the First GDPR Fines, BakerMcKenzie (Dec. 19, 2018), https://www.bakermckenzie.com/en/insight/publications/2018/12/takeaways-from-the-first-gdpr-fines.

Data Protection Commission has opened 15 investigations that specifically look at the data practices of major American technology companies, including Apple, Twitter, LinkedIn, and Facebook. (10 of these investigations are specifically focused on Facebook, including the access and portability rights, legal basis for processing in Instagram and WhatsApp, and data security incidents reported by Facebook.)[48]

French and German regulators have been aggressively focused on the activities of Google and Facebook. In January, the CNIL imposed a fine of €50 million (approximately $57 million) against Google, alleging a lack of transparency, inadequate information, and a lack of valid consent with respect to Google's advertising activities.[49] Informed consent is one of the core legal bases for processing data under the GDPR, but the CNIL notes that "it is not possible to be aware of the plurality of services, websites, and applications involved in these processing operations (Google search, YouTube, Google home, Google maps, Playstore, Google pictures…) and therefore of the amount of data processed and combined."[50] The CNIL expressed further concern with the "severity of the infringements" of essential elements of transparency, information, and consent under the GDPR, and alleged that Google was in "continuous breach[] of the Regulation."[51] Google is appealing the decision.

In February, the German Bundeskartellamt (FCO), a national competition authority, imposed restrictions on Facebook's ability to combine user data from different sources into one profile.[52] Specifically, absent "voluntary consent" from individuals, Facebook will no longer be allowed to combine data collected from WhatsApp, Instagram, and other third-party websites and apps. Competition regulators were concerned that Facebook could use its market power to obtain detailed user profiles, and that Facebook's terms of service and data use policies violated the GDPR. Facebook disagrees and has argued that "GDPR specifically empowers data protection regulators – not competition authorities – to determine whether companies are living up to their responsibilities."[53]

---

[48] Irish Data Protection Commission, Annual Report: 25 May - 31 December 2018, available at https://www.dataprotection.ie/sites/default/files/uploads/2019-02/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf.

[49] CNIL, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[50] Id.

[51] Id.

[52] Press Release, Bundeskartellamt prohibits Facebook from combining user data from different sources (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[53] Yvonne Cunnane, Why We Disagree With the Bundeskartellamt, Facebook (Feb. 7, 2019), https://newsroom.fb.com/news/2019/02/bundeskartellamt-order/.

Both disputes are likely to result in court battles, but they suggest that regulators intend to aggressively use the GDPR to police the data collection, use, and sharing practices of internet giants. More broadly, these regulatory actions underscore the need for the US to adopt its own data protection regime. Doing nothing is not an option. If the US does not act it will cede control over these decisions to the EU and be largely bound by the decisions of those regulators.

IV. California Consumer Privacy Act is Still In Flux

While Congress has long debated the merits of a federal privacy law, the California Consumer Privacy Act (CCPA) was enacted rapidly. The speed with which the CCPA was signed into law — and the reasons why such speed were necessary — is a lesson on how hard it can be to push forward strong privacy laws.[54] It has forced companies to acknowledge that the status quo is untenable and that some fundamental business practices need to change.

While the CCPA is often referred to as a "Californian GDPR," this is inaccurate. While there are significant similarities between the GDPR and CCPA, the CCPA is not a comprehensive privacy framework. The GDPR includes both individual rights, as discussed above, and accountability mechanisms (including requirements that companies engage in privacy by design, undertake data protection impact assessments, document their processing activities, and employ independent privacy officers) to encourage companies to embrace data minimization and purpose specification when they use data. In contrast, there are several provisions in the CCPA that actually promote expansive uses of information by businesses. Companies have basically unlimited rights to use personal information for businesses purposes. There are no actual restrictions on data collection.[55]

Instead, the CCPA is largely focused on transparency and offering tools to help Californians stop companies from sharing and selling their personal information. The core features of the CCPA include:

- A right to know about what personal information a business has about them, and where categories of that personal information come from or are sent;
- A right to access the "specific pieces" of personal information a company has about them (and an implicit endorsement of a data portability right);

[54] Kashmir Hill, California Has 48 Hours to Pass This Privacy Bill or Else, Gizmodo (June 26, 2018), https://gizmodo.com/california-has-48-hours-to-pass-this-privacy-bill-or-el-1827117016.
[55] For a high level comparison of the GDPR with the CCPA, see Joseph Jerome, California Privacy Law Shows Data Protection on the March, ABA Antitrust, Vol. 33:1 (2018).

- A right to delete personal information that a business has collected from them. Importantly, while the above rights apply to all information a business has collected about a consumer, the deletion right applies only to information collected from an individual;
- A right to opt out of the sale of personal information about them. For minors under the age of 16, businesses must not knowingly sell personal information without obtaining consent (either parental consent for minors under 13 or the consent of minors aged 13-16); and
- A right to receive equal service and pricing from a business if an individual exercises her privacy rights under CCPA.[56]

Companies that have already prepared for the GDPR will be in a better position to navigate California's law as it evolves, but the CCPA will likely force companies such as U.S.-focused advertisers and the offline data ecosystem that have been able to ignore EU's data protection trends to step up their privacy protections.[57]

While the CCPA has dominated debates about commercial data privacy in the United States in recent months, the reality is that it is too soon to know the full impacts of the law. However, we should recognize that to the extent that companies claim to support a federal law that would be "stronger" than California's, most of the industry proposals on the table do not match what is being discussed at the state level.[58]

V. Moving Beyond Notice and Consent

Existing privacy regimes including GDPR and CCPA rely too heavily on the concept of notice and consent, placing an untenable burden on consumers and failing to rein in harmful data practices.[59] 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

[56] See Californians for Consumer Privacy, About the California Consumer Privacy Act, https://www.caprivacy.org/about (last visited Mar. 10, 2019).
[57] See Bradley Barth, Meeting GDPR standards doesn't guarantee Calif. privacy law compliance, experts warn, SC (Mar. 8, 2019), https://www.scmagazine.com/home/security-news/meeting-gdpr-standards-doesnt-guarantee-calif-privacy-law-compliance-experts-warn/; Future of Privacy Forum, CCPA, face to face with the GDPR: An in depth comparative analysis (Nov. 28, 2018), https://fpf.org/2018/11/28/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/.
[58] Omer Tene, Twitter (Mar. 7, 2019), https://twitter.com/omertene/status/1103698390452457472.
[59] 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).

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.[60] Further, people operate under woefully incorrect assumptions about how their privacy is protected.[61] 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.[62]

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.[63] 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.

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.[64] 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

[60] Grauer, *supra* note 5.
[61] 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.
[62] 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.
[63] 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/.
[64] Press release, FTC, Feb. 28, 2018, https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

disclosure, users purportedly consented to disclosing information by filling out a quiz, but had no way of foreseeing how that information would be used.[65]

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."[66] 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.

VI. What U.S. 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, 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.[67]

Individual Rights in Data

[65] 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.

[66] 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.

[67] 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.

A federal law must include basic rights for individuals to access, correct, delete, and port their personal data.[68] 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."[69] This information can be used to target vulnerable consumers with potentially harmful offers, such as payday loans.[70]

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 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.[71] With appropriate, tailored exceptions, these provisions can be crafted in a

---

[68] 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/.

[69] 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.

[70] *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.

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

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.

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.[72] 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.[73]

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.[74]

[72] 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.

[73] *Id.*

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

- 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.[75]
- 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.[76]
- Advertisers have leveraged data to target risky, undesirable, or even fraudulent opportunities based on sensitive characteristics.[77] 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.[78]
- The payday loan and for-profit college industries have used sensitive segments as well as deceptive data collection interfaces to generate leads.[79]

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.

---

[75] 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.

[76] *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/.

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

[78] 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.

[79] Upturn, *supra* note 25.

Funding for the agency has fallen five percent since 2010, and its resources are strained.[80] 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.[81] 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.[82] 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.[83]

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.[84] 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.

---

[80] 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.

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

[82] 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.

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

[84] 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.