Statement of Caitriona Fitzgerald

Deputy Director, Electronic Privacy Information Center (EPIC)

Hearing on "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security"

Before the

House Committee on Energy & Commerce
Subcommittee on Consumer Protection and Commerce
United States House of Representatives

June 14, 2022

Chair Schakowsky, Ranking Member Bilirakis, and members of the Subcommittee, thank you for holding this hearing and for the opportunity to testify today on the American Data Privacy and Protection Act. My name is Caitriona Fitzgerald, Deputy Director at the Electronic Privacy Information Center, or EPIC. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.

For more than two decades, powerful tech companies have been allowed to set the terms of our online interactions. Without any meaningful restrictions on their business practices, they have built systems that invade our private lives, spy on our families, and gather the most intimate details about us for profit. These companies have more economic and political power than many countries and states. Through a vast, opaque system of databases and algorithms, we are profiled and sorted into winners and losers based on data about our health, finances, location, gender, race, and other personal characteristics and habits. The impacts of these commercial surveillance systems are especially harmful for marginalized and multi-marginalized communities, fostering discrimination and inequities in employment, government services, health and healthcare, education, and other life necessities.

But it does not have to be this way – we can have a strong technology sector in the United States while protecting personal privacy. We need to retake control of our personal information from the entities that want to collect it, use it, and disclose it for any and every purpose they choose. We do not need any more evidence that self-regulation by technology companies does not work. The result of lack of regulation is clear and it has put us in this crisis. The longer Congress delays, the more difficult it will be to rein in these harmful business practices. It is long past time to establish comprehensive protections for privacy and civil rights online. Congress must act now to reclaim privacy as a meaningful right and to protect personal data. The American Data Privacy and Protection Act presents Congress with the best opportunity it has had in decades to stop the very real harms that are happening online every minute of every day.

In my testimony I will discuss the crisis we face today due to the lack of a comprehensive U.S. privacy law, how the American Data Privacy and Protection Act addresses that crisis, and some opportunities to improve the bill.

A. The United States' Data Privacy Crisis: Surveillance Capitalism Run Wild

The United States now faces a data privacy crisis. The lack of a comprehensive U.S. privacy law has allowed abusive data practices to flourish, threatening our rights and institutions. Robust data protection standards are essential to ensure the preservation of human rights and dignity and the healthy functioning of our democracy.

Due to the failure of policymakers in the United States to establish adequate data protection standards, online firms have been allowed to deploy commercial surveillance systems that collect and commodify every bit of our personal data.[1] The platforms and data brokers that track us across the internet and build detailed profiles to target us with ads also expose us to ever-increasing risks of breaches, data misuse, manipulation, and discrimination.[2]

The notice-and-choice approach to privacy regulation that dominated the United States' response to this uncontrolled data collection over the last three decades simply does not work. The focus on notice has led to longer and more complicated privacy policies that users do not read and could not change even if they did. And modern surveillance systems, including the schemes used to track our digital and physical activities across the web and across devices, are too complex and opaque for the vast majority of internet users to understand or control.

BuzzFeed recently reported that religious social networking service and app Pray.com was collecting detailed information about its users, including the texts of their posts, and linking it with information obtained from third-parties and data brokers.[3] Pray.com was also releasing detailed data about its users with third-parties, including Facebook, meaning "users could be targeted with ads on Facebook based on the content they engage with on Pray.com — including content modules with titles like 'Better Marriage,' 'Abundant Finance,' and 'Releasing Anger.'"[4] Users of the app called these practices "exploitative," "manipulative," and "predatory," and said they went against the private nature of prayer.[5]

In 2020, The Markup found that one-third of websites surveyed contained Facebook's tracking pixel, which allows Facebook to identify users (whether or not they are logged into Facebook) and connect those website visits to their Facebook profiles.[6] The Markup also scanned hundreds of websites on sensitive topics and discovered an alarming volume of tracking, including:

- A state agency page on how to report child abuse sending data about its visitors to six ad tech companies;
- WebMD and Everyday Health sending visitor data to dozens of marketing companies; and

[1] *See generally* Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019).
[2] *See* Consumer Fed. of America, *Factsheet: Surveillance Advertising: How Does the Tracking Work?* (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-how-tracking-works/.
[3] Emily Baker-White, *Nothing Sacred: These Apps Reserve The Right To Sell Your Prayers*, BuzzFeed (Jan. 25, 2022), https://www.buzzfeednews.com/article/emilybakerwhite/apps-selling-your-prayers.
[4] *Id.*
[5] *Id.*
[6] Julia Angwin, *What They Know… Now,* The Markup (Sept. 22, 2020), https://themarkup.org/blacklight/2020/09/22/what-they-know-now.

- The Mayo Clinic using key logging to capture health information individuals typed into web forms for appointments and clinical trials, regardless of whether the individual even submitted the form or not—information which was saved to a folder titled "web forms for marketers/tracking."[7]

These trackers collect millions of data points each day that are sold or transferred to data brokers, who then combine them with other personal data sources to build invasive profiles. Often these profiles are used to target people with "personalized" advertisements that stalk them across the web. In other cases these profiles are fed into secret algorithms used to determine the interest rates on mortgages and credit cards, to raise consumers' interest rates, or to deny people jobs, depriving people of opportunities and perpetuating structural inequalities.[8]

B. Data Minimization is Critical in Limiting Unfettered Data Collection

The ubiquitous online surveillance described above causes substantial and widespread privacy harms. Data minimization offers a solution. Data minimization sets limits on processing which requires data to be used *specifically* to deliver the goods and services that an individual has requested, consistent with the consumer's expectations. Companies complying with data minimization requirements must also delete personal information when it is no longer needed to serve the purpose for which it was collected.

Section 101 of the American Data Privacy and Protection Act establishes limits on the unfettered processing of personal data by requiring that entities only collect, use, and transfer data that is reasonably necessary, proportionate, and limited to: (1) provide a specific product or service requested by the individual or (2) a communication reasonably anticipated within the context of the relationship, with some exceptions specifically spelled out in section 209. The adoption of data minimization techniques consistent with this rule is essential to data protection across the board.[9]

Data minimization is essential for both consumers and businesses. Data minimization principles provide much needed standards for data security, access, and accountability, assign responsibilities with respect to user data, and restrict data collection and use. Indeed, a data

---

[7] Aaron Sankin & Surya Mattu, *The High Privacy Cost of a "Free" Website*, The Markup (Sept. 22, 2020), https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites.

[8] *See Protecting Consumer Privacy in the Age of Big Data*, 116th Cong. (2019), H. Comm. on the Energy & Comm., Subcomm. on Consumer Protection and Comm. (Feb. 26, 2019) (testimony of Brandi Collins-Dexter, Color of Change), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Brandi%20Collins%20Dexter%2002.26.2019.pdf.

[9] *See* EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/; *see also* Access Now, *Data minimization: Key to protecting privacy and reducing harm* (May 2021), https://www.accessnow.org/data-minimization-guide/.

minimization rule can provide clear guidance to businesses when designing and implementing systems for data collection, storage, use, and transfer. And data security will be improved because personal data that is not collected in the first place cannot be at risk of a data breach.

Data minimization is not a new concept; it just needs to be applied as a rule to all personal data collection online. Privacy laws dating back to the 1970s have recognized and applied this concept. The Privacy Act of 1974, a landmark privacy law regulating the personal data practices of federal agencies, requires data minimization. Each agency that collects personal data shall "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[10]

The recently passed update to the California Consumer Privacy Act also includes provisions requiring a limited form of data minimization.[11] The European Union General Data Protection Regulation (GDPR) requires companies, among other things, to minimize collection of consumer data to what is "[a]dequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."[12] This means that many companies that would be covered by this bill are already complying with data minimization rules for users in other jurisdictions.

Human beings are more than data points to be sold to advertisers and data brokers. We all deserve privacy and autonomy with respect to our personal information. Individuals should be allowed to browse the internet or scroll through their favorite apps without worrying whether companies will use their own data in ways they do not anticipate. Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data. EPIC encourages the Subcommittee to retain the data minimization provisions in section 101 of the bill and to pair them with a duty of loyalty that will require companies to act in the best interest of the individuals whose data they collect.[13]

C. Some Forms of Sensitive Data Uses Deserve Even Higher Protections

Some types and uses of data are especially sensitive and warrant even stricter regulation. For instance, biometric, genetic, and precise geolocation data are inherently sensitive. But even information about the products people buy and the services they search for can qualify as

[10] 5 U.S.C. § 552a (e)(1).
[11] Cal. Civ. Code § 1798.100(c).
[12] Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 § 1(c).
[13] *See* Neil M. Richards & Woodrow Hartzog, *Legislating Data Loyalty*, (June 8, 2022). 97 Notre Dame L. Rev. Reflection 356 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4131523.

sensitive if used to make inferences about individuals' health, religious beliefs, economic situations, and other characteristics.

Nearly every week there is a new story about how precise location data is being packaged and sold to the highest bidder. Location data can be combined with other data to reveal an individual's movements or to track them in real time, which can pose a significant threat to physical safety. Location data can also reveal sensitive information about individuals including their religious affiliation, their personal and political beliefs, their sexual orientation, their health status, or other sensitive categories. Despite common assurances from companies, precise location data is not "anonymous" and can in many cases be linked back to an individual. Last year, a top Catholic Church official was forced to resign after a Catholic media site used cellphone data to show that the priest was a regular user of the queer dating app Grindr and visited gay bars.[14] Both Google[15] and location data firms[16] have been found harvesting users' locations even after they have opted out. The Centers for Disease Control paid $420,000 to access one year of location data from data broker SafeGraph to track patterns of tens of millions of Americans during the COVID-19 pandemic.[17]

Health data is another category of data that requires heightened protection. Many people assume that the health data they enter in apps is protected by the Health Information Portability and Accountability Act (HIPAA), but it is frequently not. HIPAA only covers health care providers, health insurers, and health care clearinghouses. Last year, Flo Health, the developer of a popular fertility-tracking app, settled a Federal Trade Commission complaint alleging that the company shared health information of its users with outside data analytics providers, including Facebook and Google, after promising such information would be kept private.[18] But the only reason the FTC was able to bring a case against the company is that Flo Health misled users in its privacy policy, stating that the company and app would not share users' health details with anyone. If Flo Health had simply disclosed these practices in their privacy policy, there would be no federal law expressly prohibiting the company from transferring users' sensitive fertility data to marketers and third parties.

---

[14] Michelle Boorstein et al., *Top U.S. Catholic Church official resigns after cellphone data used to track him on Grindr and to gay bars*, Wash. Post (July 21, 2021), https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/.
[15] Ryan Nakashima, *Google tracks your movements*, like it or not, Assoc. Pres (Aug. 13, 2018), https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb.
[16] Joseph Cox, *Location Data Firm Got GPS Data From Apps Even When People Opted Out*, Vice (Oct. 25, 2021), https://www.vice.com/en/article/5dgmqz/huq-location-data-opt-out-no-consent.
[17] Joseph Cox, *CDC Tracked Millions of Phones to See If Americans Followed COVID Lockdown Orders*, Vice (May 3, 2022), https://www.vice.com/en/article/m7vymn/cdc-tracked-phones-location-data-curfews.
[18] *In re Flo Health, Inc.*, FTC File No. 192-3133 (June 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

The American Data Privacy and Protection Act rightly recognizes that some sensitive categories and uses of data deserve stricter controls and would halt some of these dangerous business practices. Section 204 requires that, on top of meeting the data minimization threshold, a covered entity may not collect, process, or transfer an individual's sensitive personal data without affirmative express consent. And for some categories of data—including precise geolocation data, social security numbers, biometric information, and genetic data—section 102 prohibits transfers outright or restricts them to very limited circumstances.

The concern with sensitive data is that it can easily be misused and causes significant harm if breached. U.S. privacy law should strictly limit the collection, use, and transferring of sensitive data.

D. Algorithmic Oversight is Particularly Important in Mitigating Harms to Marginalized Communities

The use of artificial intelligence and other automated systems to make decisions about individuals poses significant risks to fundamental rights. Public and private actors are increasingly relying on automated decision-making tools to determine eligibility for jobs, education, housing, parole, bail, credit, insurance, healthcare, and government services.[19] The error, bias, and discriminatory patterns embedded in these systems perpetuate systemic inequality,[20] yet neither public agencies nor private companies are typically required to evaluate the impacts and biases of these systems before they use them.

Indeed, many automated decision-making systems have been deployed by both government agencies and private companies with little to no oversight, despite questions regarding their effectiveness.[21] A 2019 National Institute of Standards and Technology ("NIST") study of facial recognition tools—which are typically "AI-based"[22]—found that the systems were up to 100 times more likely to return a false positive for a non-white person than for a white person.[23] Specifically, NIST found that "for one-to-many matching, the team saw higher rates of false positives for African American females," a finding that is "particularly important

---

[19] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).
[20] *See* Rashida Richardson, *Racial Segregation and the Data-Driven Society: How Our Failure to Reckon with Root Causes Perpetuates Separate and Unequal Realities*, 36 Berkeley Tech. L.J. 3 (2022).
[21] David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey, & Mariano-Florentino Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* 6 (Feb. 2020), https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf.
[22] Nat'l Inst. Standards & Tech., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* 14 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[23] Nat'l Inst. Standards & Tech., *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

because the consequences could include false accusations."[24] A separate study by Stanford University and MIT, which looked at three widely deployed commercial facial recognition tools, found an error rate of 34.7% for dark-skinned women compared to an error rate of 0.8% for light-skinned men.[25] A review of Rekognition—an Amazon-owned facial recognition system marketed to law enforcement—revealed indications of racial bias and found that the system misidentified 28 members of U.S. Congress as convicted criminals.[26] This type of facial recognition is used in public benefit verification, job applicant screening tools, remote test proctoring systems, and numerous other sensitive contexts.

Consumers are often surprised to learn that decisions impacting their lives[27] were made using algorithms. In healthcare settings, consumers have been shocked to discover that data collected by their essential health equipment was used to make reimbursement decisions.[28] Insurance firms have fed patients' financial investment data, car ownership records, cell phone numbers, and property records into algorithms to predict health outcomes and generate health risk scores.[29]

Even our children are not safe from having decisions made about them by opaque algorithms. The Markup recently released results from an extensive investigation of software used in K-12 schools. One company, PowerSchool, was found to be using algorithms that relied on indicators of family wealth, such as free and reduced lunch status, to "predict" a student's

---

[24] *Id*.

[25] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1–15 (2018), https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/.

[26] Russell Brandom, *Amazon's facial recognition matched 28 members of Congress to criminal mugshots*, The Verge (July 26, 2018), https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

[27] *See* Genevieve Smith & Ishita Rustagi, *When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity*, Stan. Soc. Innov. Rev. (Mar. 31, 2021), https://ssir.org/articles/entry/when_good_algorithms_go_sexist_why_and_how_to_advance_ai_gender_equity ("A husband and wife compared their Apple Card spending limits and found that the husband's credit line was 20 times greater. Customer service employees were unable to explain why the algorithm deemed the wife significantly less creditworthy.").

[28] *See* All Things Considered, *How Insurers Are Profiting Off Patients With Sleep Apnea*, NPR (Nov. 21, 2018), https://www.npr.org/2018/11/21/670142105/how-insurers-are-profiting-off-patients-with-sleep-apnea ("And that's when he realized that the machine was actually spying on him and tracking his sleep habits and sleep patterns. And the irony is he wasn't able to use the machine because he didn't have the new mask and yet they hadn't been sending the new mask because they said he wasn't using the machine.").

[29] *See* Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*, ProPublica (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

future success and provide teachers with graduation risk scores as early as seventh grade.[30] PowerSchool claims to have data on 75% of K-12 students in North America.[31]

The Markup also examined Naviance software, which is used by approximately two-thirds of high school students in the U.S. to research and apply to college. Naviance was found to gather data on students as they used the software and to allow colleges to target students with paid advertisements promoting enrollment.[32] The Markup obtained contracts showing that numerous universities, including the University of Kansas, University of Southern Maine, and the University of Massachusetts Boston used the software to target their enrollment ads only to white students.[33]

These data practices threaten individual privacy and civil rights, and companies have proven time and again that they cannot police themselves.[34] The provisions of the American Data Privacy and Protection Act that extend civil rights protections online and provide oversight of algorithms are vital to protecting the public, especially marginalized individuals and communities.

The American Data Privacy and Protection Act sets accountability and transparency requirements for automated decision-making tools by requiring Algorithmic Impact Assessments and Algorithm Design Evaluations, which can provide meaningful oversight if done right.[35] EPIC does recommend adding more robust requirements to the impact assessments under section 207 so they do not simply become box-checking exercises.[36] Compelling businesses to explain how each algorithm was developed, the training data, and the anticipated purposes and capabilities would make these assessments more effective.

Unless express, binding limits on the use of AI are established *now*, the technology will quickly outpace our collective ability to regulate it. Effective algorithmic impact assessments

---

[30] Todd Feathers, *This Private Equity Firm Is Amassing Companies That Collect Data on America's Children*, The Markup (Jan. 11, 2022), https://themarkup.org/machine-learning/2022/01/11/this-private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children.

[31] *Id.*

[32] Todd Feathers, *College Prep Software Naviance Is Selling Advertising Access to Millions of Students*, The Markup (Jan. 13, 2022), https://themarkup.org/machine-learning/2022/01/13/college-prep-software-naviance-is-selling-advertising-access-to-millions-of-students.

[33] *Id.*

[34] *See generally* Ari Ezra Waldman, *Industry Unbound* (2021) (demonstrating that many privacy impact assessments conducted under GDPR have become little more than checkbox forms).

[35] *See* Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 Fordham L. Rev. 613, 624 (2019), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5633&context=flr ("Procedural requirements like algorithmic impact assessments, source code transparency, explanations of either the result or the logic behind it, and a human in the loop who can hear someone's appeal move opaque automated systems closer to more familiar, and more accountable, decision-making regimes.")

[36] *Id.* at 628 (citing Lauren Edelman, *Working Law: Courts, Corporations, and Symbolic Civil Rights* 100-50 (2016)).

with strong oversight are critical to protect against discriminatory uses of data and ensure fairness in decision-making.

E. Strong Enforcement is Critical to Privacy Protection

Robust enforcement is the bedrock of effective privacy protection. This means both a private right of action and enforcement by authorities at the federal and state levels—including the authorities that are best suited to tackle data protection.

1. A Private Right of Action

A private right of action is a crucial tool to supplement administrative enforcement, and we applaud the drafters of this bill for coming to a workable compromise on a private right of action. If a company violates federal privacy law, affected individuals and groups of individuals should be able to pursue meaningful redress from that company on their own. While government enforcement is essential, the scope of data collection online is simply too vast for one entity—or even 50 entities—to regulate. Individuals and groups of individuals who use online services are in a good position to identify privacy issues and bring actions to vindicate their interests. In the absence of a private right of action, there is a very real risk that companies will not comply with the law because they think it is unlikely that they will be caught or fined. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations.

Many privacy laws include a private right of action, and these provisions have historically made it possible to hold companies accountable for their privacy violations. Though the American Data Privacy and Protection Act does not include statutory damages, in the past Congress has frequently included statutory damages in privacy statutes to avoid protracted disputes over quantifying damages. This is important because it is often difficult to assign a specific economic value to the harm caused by a privacy violation.

For example, when Congress passed the Cable Communications Policy Act in 1984, it established privacy rights for cable subscribers and created a private right of action for recovery of liquidated damages of $100 per for violation or $1,000, whichever is higher.[37] The Video Privacy Protection Act specifies liquidated damages of $2,500.[38] The Fair Credit Reporting Act affords individuals a private right of action that can be pursued in federal or state court against credit reporting agencies, users of credit reports, and furnishers.[39] In certain circumstances, individuals can also recover attorney's fees, court costs, and punitive damages. The Driver's

[37] 47 USC § 551(f).
[38] 18 USC § 2710(c)(2).
[39] 15 U.S.C. §§ 1681n-1681o.

Privacy Protection Act similarly includes a private right of action.[40] The Telephone Consumer Protection Act allows individuals who receive unsolicited telemarketing calls to recover actual monetary loss or up to $500 in damages per violation.[41]

The statutory damages set by federal privacy laws are not large in an individual case, but they can provide a powerful incentive in large cases and are necessary to ensure that privacy rights will be taken seriously by businesses that process personal data. EPIC encourages the Subcommittee to add statutory damages to the private right of action in section 403.

2. Federal Agency Enforcement

Federal agency enforcement is also critical. EPIC has long advocated for the creation of a standalone Data Protection Agency,[42] but establishing a bureau within the Federal Trade Commission is a step in the right direction, provided Congress allocates adequate resources to the new bureau so the FTC can carry out all the regulatory and enforcement obligations required of the Commission in this bill.

We applaud the provisions in the American Data Privacy and Protection Act giving the FTC first-time civil penalty authority. Existing law severely constrains the Commission's power to impose financial consequences on companies that violate civil and privacy rights. Unless a company is already under an FTC consent decree, the Commission can generally only obtain civil penalties if a business violates a cease-and-desist order or a trade regulation rule, both of which require a lengthy administrative process. Enabling the Commission to seek civil penalties against first-time violators will be a powerful deterrent against exploitative data practices and a key tool for holding lawbreaking companies accountable.

Rulemaking authority is also a cornerstone of effective data protection. Although the right to privacy is timeless, the ways that companies seek to use personal data and the technologies that process it are rapidly changing. Safeguarding the right to privacy in the internet era requires clear, detailed, and up-to-date rules developed with the benefit of public participation and agency expertise. It is critical that Congress give the FTC the authority to implement the American Data Privacy and Protection Act through public rulemaking processes. Rulemaking authority will enable the Commission to clarify the obligations of covered entities and the rights of individuals, to update those rules as technology and circumstances evolve, and to effectuate the purposes of the Act with input from all stakeholders.

---

[40] 18 U.S.C. § 2724.
[41] 47 USC § 227(c)(5).
[42] *See Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors*, 117th Cong. (2021), H. Comm. on H. Admin. (Feb. 16, 2022) (testimony of Caitriona Fitzgerald, EPIC), https://epic.org/wp-content/uploads/2022/02/EPIC-HouseAdmin-Feb2022.pdf.

As drafted, the Act includes FTC rulemaking authority to define new categories of sensitive covered data responsive to emerging privacy threats; to establish processes for access, correction, and deletion requests by individuals; to create a global mechanism enabling individuals to opt out of certain abusive data practices industry-wide; and to implement the Act's data security requirements. We support these provisions and urge Congress to ensure that the FTC has the power to implement other critical components of the Act through rulemaking, including the data minimization, duty of loyalty, and preemption sections.

3. Enforcement by State Attorneys General and Agencies

State Attorneys General have historically played a strong role in privacy enforcement, largely stemming from their consumer protection watchdog role.[43] The American Data Privacy and Protection Act rightly preserves and expands this critical enforcement role for state Attorneys General. The bill should also recognize that states may have specialized privacy enforcement agencies and should not limit authority specifically to the "attorney general of a State or the chief consumer protection officer."

F. It Is Time for the United States to Reclaim Its Role as a Global Leader for Privacy Protection

It is long past time for the United States to enact a comprehensive privacy regime and reclaim our role as a global leader in protecting individuals' fundamental rights to privacy and data protection.

Many who read about emerging privacy threats today think of how they will be analyzed under Europe's General Data Protection Regulation or even the emerging regulatory frameworks being developed in California, Colorado, and other states. But it was the United States Congress that stepped forward in the 1970s to tackle the emerging issues of records, computers, and the rights of citizens;[44] to address the threat of unfair and inaccurate consumer profiles; and to call for closer study of how to protect personal privacy in an information society.[45] And many decades before those more modern laws were passed, the very concept of privacy as an individual right was pioneered here in the United States by Louis Brandeis and Samuel Warren[46] and ultimately developed and implemented through state common law.[47] Even in the earliest

[43] Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747 (2017), https://scholarship.law.nd.edu/ndlr/vol92/iss2/5/.
[44] U.S. Dep't of Health, Educ. & Welfare, Records, Computers, and the Rights of Citizens (1973), *available at* https://epic.org/documents/hew1973report/.
[45] U.S. Privacy Protection Study Comm'n, Personal Privacy in an Information Society (1977), *available at* https://archive.epic.org/privacy/ppsc1977report/.
[46] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. R. 193 (1890).
[47] William L. Prosser, Privacy, 48 Calif. L. Rev. 383 (1960).

days of the development of our federal communications regulations, privacy was recognized as a critical right and enshrined in statute.[48]

Indeed, the United States' leadership on privacy and legislation to preserve the security of electronic communications helped usher in the personal computing and internet revolutions that made possible so many aspects of our modern society. And yet at critical points in the development and deployment of these powerful technologies over the last three decades, Congress failed to modernize our critical legal infrastructure. Instead, the United States sat by as other countries took a proactive approach to reining in the harmful business practices and threats to individual rights that have emerged in the internet era.

The hands-off and self-regulatory approaches to regulating privacy and data collection practices have failed. But in many cases the hard work of consumer protection agencies, state attorneys general, and consumer advocates have held back some of the most egregious data abuses. And state lawmakers filled the gaps with new laws addressing emerging data protection problems. Now it is time for Congress to give federal and state authorities and consumer advocates the tools they need to protect privacy rights online.

The United States is uniquely positioned to tackle these hard problems. Despite having a strong rights-based approach and broad geographic impact, Europe's General Data Protection Regulation has faced criticism for its indeterminacy and a lack of strong enforcement.[49] That is why it is critical for Congress to establish clear and comprehensive rules backed by robust enforcement to protect Americans online and reestablish the U.S. as a global leader in both privacy protection and technological innovation.

G. Conclusion

Privacy is a fundamental right, and it is time for Congress to act to protect the privacy rights of all Americans. The bipartisan American Data Privacy and Protection Act presents Congress with the best opportunity it has had in decades to stop the very real data abuses and privacy harms that are happening every minute of every day. EPIC urges Congress to not let this moment pass without enacting strong protections for Americans' privacy. We need comprehensive data protection legislation, robust enforcement, and ample resources to ensure privacy, equality, and security in our online world.

Thank you for the opportunity to testify today.

---

[48] *See* 47 U.S.C. § 605(a).
[49] *See, e.g.*, Ilse Heine, Ctr. for Nat'l Sec. Studies, *3 Years Later: An Analysis of GDPR Enforcement* (2021), https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement.