epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Statement of Alan Butler

Executive Director, Electronic Privacy Information Center (EPIC)

Hearing on "Protecting the Virtual You: Safeguarding Americans' Online Data"

Before the

U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law

July 30, 2025

Chair Blackburn, Ranking Member Klobuchar, and members of the Subcommittee, thank you for holding this hearing and for the opportunity to testify today on the need to better safeguard Americans' online data. My name is Alan Butler, and I am Executive Director at the Electronic Privacy Information Center. EPIC is an independent nonprofit research organization established in 1994 to secure the right to privacy in the digital age for all people.

Privacy is a fundamental right, and our laws should clearly limit the collection and use of our data and protect against abusive practices that unfairly target us based on who we are, where we have been, and what we believe. Americans deserve a law that actually protects their data online; not one that creates more check boxes or that makes them read a long contract before they order take-out or watch a news clip.

I commend this subcommittee for taking on the important work of analyzing these problems and identifying real solutions. The status quo is untenable. If the law allows a company to scrape images of all of our faces to build a universal facial recognition database, while another company tracks every site we visit, and link we click, to build invasive profiles of us, and yet another company buys and sells a detailed log of our daily movements and activities, do we have privacy protection at all? I believe that any reasonable person would say no, and demand that our lawmakers step in to fix this broken system and unlock the endless potential of our digital ecosystem when privacy protection is built in from the ground up.

We need clear rules of the road for the digital frontier, which should include limits on the sale of our data and the use of our sensitive information, including a clear prohibition on tracking our online behavior over time and across apps and sites and strict limits on the use of our location data and biometric data. These rules will protect us from fraudsters, stalkers, and scams and put individual Americans back in control of their own personal information. Furthermore, they will encourage privacy-protective innovation that can improve and expand our online world.

EPIC has long supported a robust federal privacy standard and has been calling on Congress to pass a strong comprehensive privacy law for more than 25 years. In testimony before the Senate Commerce Committee in 2001, we said:

> [T]he time has come to make clear that the right of privacy does not end where the Internet begins. There is now the chance to establish law that will allow users to enjoy the benefits of innovation and to preserve cherished values. We have the opportunity to carry forward an American tradition that has marched side by side with the advancement of new technology. But we may not have this opportunity for long. In the absence of clear legal standards, we could easily drift into a world of privacy notices and warning labels, where every keystroke on your personal computer is quietly recorded in the database of another computer, then to be merged

with data beyond your knowledge or control. In the absence of good privacy legislation, that future seems likely.[1]

Unfortunately, Congress failed to act, and the type of invasive and pervasive tracking that we warned about 25 years ago has become widespread. The public is strongly opposed to these commercial surveillance practices; recent surveys show more than 80% of Americans are concerned about how companies use their data.[2] In the absence of action by Congress, states have advanced general privacy laws with varying degrees of protection. As this Subcommittee considers federal privacy legislation, it should learn from and improve upon existing state laws with a focus on establishing clear rules that provide strong substantive protection to individuals by restricting unfair and abusive data practices.

It would be a disaster to enact a weak federal law that authorizes existing commercial surveillance practices under a "transparency" and implied "consent" model. This notice and choice approach to privacy has failed, and any work on privacy legislation in 2025 should start by recognizing that premise. We are in a data privacy crisis that is being supercharged by the rapid development and deployment of artificial intelligence. Our sensitive information is available to the highest bidder, and these data points are used against us to build detailed profiles, increase the prices we pay, and deny us access to benefits, housing, and employment. Our internet ecosystem is dominated by firms that profit directly off this ecosystem of surveillance capitalism.

States have already started this important process of advancing digital rights in the information age, and in my testimony today, I will summarize the highlights of the current state of state privacy and describe the areas where federal leadership would be most impactful.

THE STATE OF STATE PRIVACY LAWS

As Congress considers developing a federal comprehensive privacy law, it is important to understand the current state of state privacy laws. Nineteen states have passed some form of general privacy law since 2018.[3] California was the first, enacting the California Consumer Privacy Act in 2018 following a citizen-led ballot initiative.[4] That law was updated in 2020 when

[1] *Information Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Trans.*, 107th Cong. (2001) (testimony of Marc Rotenberg, Exec. Dir., EPIC), https://archive.epic.org/privacy/internet/testimony_0701.html.
[2] Colleen McClain, Michelle Faverio, Monica Anderson & Eugenie Park, *How Americans View Data Privacy,* Pew Rsch. Ctr., (Oct. 13, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[3] *US State Privacy Legislation Tracker*, Int'l Ass'n of Privacy Prof'ls (last updated July 7, 2025), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[4] Cal. Civ. Code § 1798.100.

voters approved a second ballot question to strengthen the law and establish the California Privacy Protection Agency.[5] Meanwhile, a broad range of stakeholders was giving input on the proposed Washington Privacy Act in 2019, and Big Tech companies made a huge lobbying push to weaken that proposal.[6] That bill did not ultimately pass in Washington, but it did become the model that industry successfully urged other states to adopt.

Virginia became the second state in the nation to pass a comprehensive consumer data privacy law in 2021 when it adopted the Virginia Consumer Data Protection Act based on the industry-influenced Washington Privacy Act.[7] On first read, it might seem that this law shares a lot in common with the bills Congress has deliberated on over the last five years: the American Data Privacy and Protection Act[8] and the American Privacy Rights Act.[9] Unfortunately, the exceptions swallow the rules in Virginia's law. The limits on collection and processing of data are tied to the disclosed purposes. Companies can collect any data they want, and process it for whatever purpose they chose, so long as they disclose what they are doing somewhere in a privacy policy. That isn't privacy protection, it is legal license to steal our data.

The law does prohibit any processing of sensitive data without consent, but the definition is very narrow, and the law specifically exempts the processing of pseudonymous data (e.g. digital identifiers that companies use to track and profile individuals). While Virginia residents can, in theory, request companies delete their data, the law requires them to submit requests one at a time to the hundreds—if not thousands—of entities holding their information. And because the law allows companies to sell and transfer data to third parties and to data brokers, most consumers do not have any way to know or to contact the various entities using their data. Meanwhile, Virginians also have no ability to hold companies accountable in court for violating the privacy law meant to protect them.

---

[5] *California Voters Pass the California Privacy Rights Act*, JD Supra (Nov. 13, 2020), https://www.jdsupra.com/legalnews/california-voters-pass-the-california-34997/.

[6] Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, Protocol (Feb. 19, 2021), https://web.archive.org/web/20240218235654/https://www.protocol.com/policy/virginia-maryland-washington-big-tech; Mark Scott, *How Lobbyists Rewrote Washington State's Privacy Law*, Politico (Apr. 2019), https://www.politico.eu/article/how-lobbyists-rewrote-washington-state-privacy-law-microsoft-amazon-regulation/.

[7] Jeffrey Datin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show,* Reuters (Nov. 19, 2021), https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/.

[8] H.R. 8152 (2021).

[9] H.R. 8818 (2021).

Unfortunately for consumers, Big Tech then pushed this model across the country, leading to 16 other states enacting laws largely based on Virginia's model.[10] In a recent report by EPIC and the U.S. PIRG Education Fund scoring the 19 state privacy laws, eight received Fs, and none received an A.[11]

But over the last year, there has been a shift toward more privacy-protective state legislation. Maryland enacted the Maryland Online Data Privacy Act in 2024, which builds on existing state laws but incorporates strong data minimization protections and a ban on the sale of sensitive data.[12] Maryland's law goes into effect in October 2025.[13] Also in 2024, the Vermont Legislature overwhelmingly passed an even stronger general privacy law that included a private right of action, but it was vetoed by the Governor.[14] Inspired by Maryland's success, 10 states have introduced privacy bills with strong data minimization rules this year. Several states that originally passed weak privacy laws based on industry-favored models have revisited and amended their laws to strengthen their protections. For example, Oregon strengthened its existing law by prohibiting the sale of precise geolocation data and minors' data.[15] Connecticut also updated its law, which originally passed in 2022, for the second time this year.[16] And not one state has passed industry's outdated model in 2025.

In the absence of federal action, states have stepped in to defend against digital abuses. But we still lack clear and enforceable standards against the most egregious forms of online tracking. Congress's failure to set federal privacy standards in the 25 years since the Federal Trade Commission and others called for action underscores that we need states to have the latitude to act and respond to new developments in the future. But Congress should lead and develop a federal standard that can provide more clarity, and robust enforcement, to bolster state laws.

ESSENTIAL PROTECTIONS IN ANY FEDERAL PRIVACY LAW

An essential component of any modern privacy law is a clear set of data minimization rules that sets standards for when data can be collected and used, which specific uses require opt-

[10] *The State of Privacy 2025: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better,* EPIC & U.S. PIRG Education Fund (Jan. 2025), https://epic.org/wp-content/uploads/2025/01/EPIC-PIRG-State-of-Privacy-2025.pdf.
[11] *Id.*
[12] Md. Code Ann. Com. Law § 14-4601.
[13] *Id.*
[14] Lisa Rathke, *Vermont Governor Vetoes Data Privacy Bill, Saying State Would Be Most Hostile to Businesses*, Assoc. Press (June 14, 2024), https://apnews.com/article/data-privacy-vermont-veto-2ab84d8705fa38cf89c428daa1dbfc54.
[15] H.B. 2008, 83d Leg. Assemb., Reg. Sess. (Or. 2025).
[16] S.B. 1295, Gen. Assemb., Jan. Sess. (Conn. 2025).

in consent, and which especially harmful data practices are prohibited (or most tightly restricted). Individual rights and disclosure provisions are relatively uniform across state and international laws, so Congress's focus should be on broad and flexible definitions, clear substantive protections that limit tracking and profiling, and robust enforcement.[17]

Data Minimization Is Critical

When consumers interact with a business online, they reasonably expect that their data will be collected and used only for the limited purpose necessary to provide the goods or services that they requested. For example, a consumer using a map application to obtain directions would not reasonably expect that their precise location data would be disclosed to third parties and combined with other data to profile them. Yet these business practices are widespread. Nearly every online interaction is tracked and cataloged to build detailed profiles that are used to target consumers with ads. Even offline, credit card purchases, physical movements, and "smart" devices in homes create countless data points that are logged and tracked without people's awareness or control. This ubiquitous online surveillance causes substantial and widespread privacy harms.

Frameworks based on the failed "notice and choice" model require entities to disclose what personal data they are collecting and how they plan to use it and presume that consumers will read and comprehend these notices and then be able to make a real decision about whether to agree to them. However, because of the realities of the power asymmetries between large companies and individual consumers and limitations on people's time and energy, "notice and choice" models are simply unworkable.

First, the "notice" portion of "notice and choice" fails to curb harmful business practices. Requiring companies to disclose their data practices does not place any real limits on what practices they can engage in. Companies should not have a limitless ability to decide how much personal data to collect, how long they can keep it, and what they can do with it. In fact, a rule that simply requires companies to disclose their self-determined purposes for data collection and use incentivizes them to list as many purposes as possible, and as broadly as possible, to cover every conceivable reason they would ever want to use your data.

The "choice" part of "notice and choice" similarly fails to protect privacy. Assuming that individuals have choice about what data practices to accept relies on two fictions about individual consent online: 1) that individuals are reading and understanding all the disclosures that companies are required to make before using a product or service and 2) that individuals have a real choice in whether to accept those policies. In reality, modern society relies on many

[17] *See* EPIC, *EPIC Feedback to House Energy & Commerce Majority Privacy Working Group* (Apr. 2025), https://epic.org/wp-content/uploads/2025/04/EPIC-PrivacyWGfeedback-Apr2025.pdf.

companies, products, apps, and services that individuals have no choice but to use, whether they know or agree with the way those companies use their data or not. The all-or-nothing decision to either accept the terms of a privacy policy or simply not access the service is not a meaningful choice.

To incentivize better data practices, any federal privacy law must include strong data minimization rules. Data minimization sets limits on processing that requires data to be collected and used as is reasonably necessary and proportionate to deliver the goods and services that an individual has requested. 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. Data minimization better aligns business practices with what consumers expect.

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 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 across the board 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. 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.[18]

In addition to featuring in federal privacy laws, data minimization is also a core principle in laws across the United States and internationally. The Maryland Online Data Privacy Act and the California Consumer Privacy Act—the two most protective state privacy laws—include provisions requiring forms of data minimization.[19] The European Union General Data Protection Regulation (GDPR) requires companies 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."[20] This means that many companies that would be covered by any privacy bill at the federal level are likely already complying with data minimization rules in other jurisdictions.

[18] 5 U.S.C. § 552a (e)(1) ("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.").
[19] Cal. Civ. Code § 1798.100; Md. Code Ann. Com. Law § 14-4607.
[20] Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 § 1(c).

The key with an effective data minimization provision is to ensure it is tied to the specific product or service requested by the individual, not simply to whatever purpose the collecting entity decides it wants to collect data for and discloses in its privacy policy.

Americans 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 able to browse the internet or scroll through their favorite websites and apps without worrying about whether companies will use their personal 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.

Heightened Protections for Sensitive Data

Because of its nature, sensitive personal information should be subject to heightened protections. 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 sensitive if used to make inferences about individuals' health, religious beliefs, economic situations, and other sensitive characteristics.

One of the most lucrative forms of sensitive personal data—and the riskiest for individuals—is location data. The location data market is a multi-billion-dollar industry centered on collecting and selling people's everyday comings and goings,[21] often collected from people's mobile devices and often without their knowledge or explicit consent.

Nearly every week there is a new story about how precise location data is being packaged and sold to the highest bidder.[22] On top of its inherent sensitivity, 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 traits. A top Catholic Church official was forced

[21] Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.
[22] *See, e.g.,* Press Release, *FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data,* Federal Trade Comm'n (Dec. 3, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data; Press Release, *FTC Order Will Ban InMarket from Selling Precise Consumer Location Data*, Federal Trade Comm'n (Jan. 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data;

to resign a few years ago 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.[23]

Apps are not the only way your location data ends up on the open market. Texas Attorney General Ken Paxton recently sued insurance giant Allstate and its subsidiary Arity for unlawfully collecting, using, and selling data about the location and movement of Texans' cell phones through software secretly embedded in mobile apps, such as Life360 and GasBuddy. In the suit, Paxton alleges that Allstate and other insurers then used the covertly obtained data to justify raising Texans' insurance rates.[24]

Health data is another category of sensitive data that requires heightened protection. Many people assume that the health data they enter into apps or track through wearable technologies is protected by the Health Information Portability and Accountability Act (HIPAA), but it is frequently not. HIPAA only covers certain personal information in the possession of health care providers, health insurers, and health care clearinghouses,[25] meaning there is no meaningful protection at all for health information on most apps or websites. Massive privacy violations have resulted from this regulatory failure.[26] This gap in protection for health information has been exacerbated by the recent rise in reliance on telehealth services. A disturbing investigation by The Markup and health publication STAT into 50 popular telehealth companies found that all but one of them were sharing personal data—sometimes sensitive health information—with Big Tech companies.[27]

---

[23] 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/.

[24] Press Release, Att'y Gen. of Texas, *Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies* (Jan. 13, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45.

[25] *Covered Entities and Business Associates,* Dep't of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[26] *See, e.g.,* Shiona McCallum & Joe Tidy, *23andMe: Profiles of 6.9 Million People Hacked*, BBC (Dec. 5, 2023), https://www.bbc.com/news/technology-67624182 (reporting that direct-to-consumer genetic testing company 23andMe suffered a hack that resulted in the personal information of almost 7 million users being breached); Press Release, Federal Trade Comm'n, *FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising* (Mar. 2, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook (announcing the Federal Trade Commission investigation into mental health and online counseling app BetterHelp for promising users their sensitive health information would be kept private and then sharing it with Facebook, Snapchat, and other third parties for advertising).

[27] Todd Feathers, Katie Palmer & Simon Fondrie-Teitler, *"Out of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, The Markup & STAT (Dec. 13,

These numerous health privacy violations also further demonstrate the inadequacies of existing state privacy laws. Most of these examples of violations would not have been illegal under state privacy laws—but even if a state privacy law technically should have prevented these incidents, research shows that entities are not consistently complying with these laws' requirements. Laws in over a dozen states require companies to obtain consent from consumers before collecting or using their sensitive data, which includes health information, yet many health websites share this information widely without consumers' knowledge or consent.[28]

Thus, any federal privacy legislation should recognize that some sensitive categories and uses of data deserve stricter controls that would halt some of these dangerous business practices. Federal privacy legislation should require the collection and use of sensitive data to be limited to what is *strictly necessary* to provide or maintain the service the consumer asked for. Layered on top of that protection, opt-in consent for some uses, such as data transfers, provides consumers with an additional layer of control while avoiding consent fatigue. Lastly, the sale of sensitive data should be prohibited.

States have recognized the unacceptable risks and incentivizes that exist in an unregulated sensitive data market, and they have led the way on protecting sensitive data, including through banning the sale of geolocation or other sensitive information,[29] adopting the "strictly necessary" standard for collection and processing of sensitive data,[30] and placing enhanced protections on the personal data of children and minors[31] and on health information.[32]

Sensitive data 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.

2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[28] Consumer Reports & Boltive, *Companies Continue to Share Health Data Despite New Privacy Laws* (Jan. 16, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf ("As our findings illustrate, on health-related websites the sharing of data with third parties seems to be the standard practice.").

[29] Md. Code Ann. Com. Law § 14-4607; H.B. 2008, 83d Leg. Assemb., Reg. Sess. (Or. 2025).

[30] Md. Code Ann. Com. Law § 14-4607.

[31] *See, e.g.,* S7694A, 2023-2024 Reg. Sess. (N.Y. 2023); Md. Code Ann. Com. Law § 14-4601; Cal. Civ. Code §§ 1798.99.28–1798.99.40; Cal. Health & Safety Code §§ 27000–27007.

[32] *See, e.g.,* H.B. 1155, 68th Leg., 2023 Reg. Sess. (Wash. 2023); S.B. 754, 2025 Reg. Sess. (Va. 2025); S.B. 370, 82d Sess., 2023 Reg. Sess. (Nev. 2023).

Ubiquitous Online Tracking Is Particularly Harmful

Much of the collection of personal data happens so routinely and automatically in the online ecosystem that consumers have little or no knowledge of its scope.[33] Tracking systems are embedded in most websites, apps, and services and begin to collect information as soon as a consumer connects. These practices are harmful to both consumers and small businesses and should be banned in any comprehensive federal privacy legislation.

BuzzFeed reported in 2022 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.[34] 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.'"[35] Users of the app called these practices "exploitative," "manipulative," and "predatory," and said they went against the private nature of prayer.[36]

This pervasive system of surveillance capitalism also raises national security concerns. A recent complaint by EPIC and Enforce alleged that Google's Real-Time Bidding (RTB) system, which dominates online advertising and operates on 33.7 million websites, 92% of Android apps, and 77% of iOS apps, sends enormous quantities of sensitive data about Americans to China and other foreign adversaries.[37]

Small businesses are harmed by these systems as well. For years, they have been told that success hinges on pouring money into online behavioral advertising, a market controlled by a handful of tech giants. They enter bidding wars against corporate behemoths. They place trackers from Big Tech giants on their websites, sending their customer data off to ad-tech companies who then turn around and use it for their own purposes, including to enrich consumer profiles

---

[33] *See* EPIC, *Online Tracking & Advertising*, https://epic.org/issues/consumer-privacy/online-advertising-and-tracking/; Jon Keegan, *Each Facebook User Is Monitored by Thousands of Companies*, Consumer Reports (Jan. 17, 2024), https://www.consumerreports.org/electronics/privacy/each-facebook-user-is-monitored-by-thousands-of-companies-a5824207467/.

[34] 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.

[35] *Id.*

[36] *Id.*

[37] EPIC & Irish Council for Civil Liberties Enforce Complaint and Request for Investigation, Injunction, Penalties, and Other Relief to the Federal Trade Comm'n, In the Matter of Google's RTB Practices (Jan. 16, 2025), https://epic.org/wp-content/uploads/2025/01/EPIC-ICCL-Enforce-In-re-Googles-RTB-Complaint.pdf; Johnny Ryan, Irish Council for Civil Liberties, *The Biggest Data Breach: ICCL Report on Scale of Real-Time Bidding Data Broadcasts in the U.S. and Europe* (2022), https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf.

then used to target ads promoting that very small business' competitors.[38] This is not a level playing field. It's a digital black hole—swallowing resources and crushing entrepreneurial spirit, all to facilitate targeted advertising that is of dubious efficacy.[39] As Check My Ads, an advocacy group founded by former advertising industry employees recently wrote to the House Energy & Commerce Committee's Privacy Working Group:

> Privacy legislation that emphasizes data minimization and transparency leads to higher-quality, more relevant data. Right now, the advertising supply chain is bloated with third-party data—often inaccurate, outdated, or collected without meaningful consent. Acxiom, one of the world's largest data brokers, even admitted their consumer data is made up of "informed guesses," with the hope it doesn't lead to credit denial or other harm. This kind of data is not only unreliable—it wastes ad spend. Privacy-focused frameworks should encourage a shift to first-party data—information voluntarily shared by users—delivering more accurate, context-rich insights. Advertising that uses high-quality data performs better. With privacy legislation in place to curb harmful data practices and enforce consent, advertisers gain access to permissioned, engaged audiences—the kind that convert and stay loyal.[40]

The debate over privacy legislation is often seen as a conflict between consumer privacy advocates on one side and Big Tech on the other. Small businesses are often caught in the middle, wanting to protect their customers' privacy but feeling reliant on the digital advertising model offered to them by ad giants. A strong data minimization standard will not prevent businesses from advertising; rather, it will encourage ad-tech providers to innovate on privacy-protective forms of advertising.

Given the harms to both consumers and small businesses by these forms of ubiquitous tracking, any federal privacy legislation should prohibit targeted advertising using personal data

---

[38] Matt Stoller, Sarah Miller & Zephyr Teachout, *Addressing Facebook and Google's Harms Through a Regulated Competition Approach*, American Economic Liberties Project 9 (Apr. 2020), https://economicliberties.us/wp-content/uploads/2020/04/Working-Paper-Series-on-Corporate-Power_2.pdf ("But as the founder of one small business put it, 'Google allows competitors to purchase ads on our trademark, blocking and misdirecting consumers from reaching our site.' In other words, Facebook and Google operate as phone directories, only when a user dials a number for a business, Facebook and Google direct the phone call to whichever third party pays them the most.").

[39] *See, e.g.,* Suzanne Smalley, *'Junk Inferences' by Data Brokers Are a Problem for Consumers and the Industry Itself*, The Record (June 12, 2024), https://therecord.media/junk-inferences-data-brokers; Nico Neumann, Catherine E. Tucker & Timothy Whitfield, *How Effective Is Third-Party Consumer Profiling and Audience Delivery?: Evidence from Field Studies*, 38 MARKETING SCIENCE 6, 913-1084 (Oct. 2, 2019).

[40] Letter from Check My Ads to House Energy & Commerce Comm. Privacy Working Group 8 (Apr. 2025), https://checkmyads.org/wp-content/uploads/2025/04/Privacy-Working-Group-RFI-Check-My-Ads-Submission.pdf.

collected across websites and over time, as was proposed in previous bipartisan federal proposals.

Enforcement

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. The scope of data collection online is too vast for government alone to regulate. This is why previous bipartisan federal proposals such as the American Data Privacy and Protection Act and American Privacy Rights Act included a three-tiered enforcement mechanism: individual, state, and federal.

Enforcement by a relevant federal agency such as the Federal Trade Commission or a new dedicated data protection agency with adequate resources is critical for carrying out the regulatory and enforcement obligations of a federal privacy law.

State Attorneys General and state consumer protection agencies have historically played a strong role in privacy enforcement, largely stemming from their consumer protection watchdog role.[41] Any federal privacy legislation should empower state Attorneys General, state privacy protection agencies, or consumer protection officers to enforce the law.

A strong federal privacy law must also include 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 the best position to identify privacy violations 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. A private right of action preserves government resources, and the threat of statutory damages is a strong motivator to incentivize compliance with the law.

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 violation or $1,000, whichever is higher.[42] The Video Privacy Protection Act specifies liquidated damages of $2,500.[43] The Fair Credit Reporting Act affords

[41] 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/.
[42] 47 USC § 551(f).
[43] 18 USC § 2710(c)(2).

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.[44] In certain circumstances, individuals can also recover attorney's fees, court costs, and punitive damages. The Driver's Privacy Protection Act similarly includes a private right of action.[45] 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.[46]

A private right of action ensures controllers have strong financial incentives to comply with privacy laws. We have seen evidence of this in Illinois,[47] where a biometric privacy law passed in 2008 includes a private right of action. Lawsuits under that law have led to changes to harmful business practices, such as forcing facial recognition company Clearview AI to stop selling its face surveillance system to private companies.[48]

In contrast, in states where Attorneys General have sole enforcement authority, we have seen little enforcement of (and compliance with) privacy laws.[49]

HOW SHOULD A FEDERAL PRIVACY LAW INTERACT WITH EXISTING LAWS?

It is important for Congress to set a strong standard now, but we cannot assume that a future Congress will be able to update that standard on a regular basis.

In privacy and consumer protection law, federal ceiling preemption is an aberration. Historically, federal privacy laws have not preempted stronger state protections or enforcement efforts. Federal consumer protection and privacy laws, as a general matter, operate as regulatory baselines and do not prevent states from enacting and enforcing stronger protections. The Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Drivers Privacy Protection Act, the

[44] 15 U.S.C. §§ 1681n-1681o.
[45] 18 U.S.C. § 2724.
[46] 47 USC § 227(c)(5).
[47] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Inst. (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf.
[48] Ryan Mac & Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition Database*, N.Y. Times (May 9, 2022), https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html.
[49] *See generally* Consumer Reports, *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws* (Apr. 2025), https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf; Consumer Reports & Boltive, *supra* note 28.

Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act all allow states to craft protections that exceed federal law.

Although the federal government has enacted several sector-specific privacy laws over the years, most privacy legislation in the United States is enacted at the state level. Many states have specific legislation on employment privacy (drug testing, background checks, employment records), Social Security Numbers, video rental data, credit reporting, cable television records, arrest and conviction records, student records, tax records, wiretapping, video surveillance, identity theft, library records, financial records, insurance records, privileges (relationships between individuals that entitle communications to privacy), and medical records. In fact, these existing laws would significantly complicate any attempt at ceiling preemption in a comprehensive federal privacy law.

Conflict preemption has been sufficient for other privacy regimes, and there is no reason that it cannot work in comprehensive federal privacy legislation. Most states already operate on a common framework, so if federal privacy legislation sets a higher floor for protections than exists in current state privacy laws, compliance with that floor will be sufficient to meet state standards and will serve as a deterrent to states to enact additional laws until changes in technology necessitate it.

CONCLUSION

I will conclude by noting that while these issues are complicated, there has been a wealth of great work done by this Committee and other Committees over the last five years to develop a strong framework. There is broad common ground about the need for robust privacy protection, and the areas of disagreement are focused on the specific boundaries that should define a comprehensive privacy law. We continue to support the development of these standards and look forward to the opportunity to provide our expertise.

Thank you again for the opportunity to testify today.