April 7, 2025

Chairman Brett Guthrie
House Energy and Commerce Committee
PrivacyWorkingGroup@mail.house.gov

Re: Request for Information to Explore Data Privacy and Security Framework

Dear Honored Members of the Energy and Commerce Committee Privacy Working Group,

Consumer Reports[1] is pleased to give feedback on the Privacy Working Group's Request for Information on potential privacy legislation. Below we provide responses to a number of the RFI's specific questions.

While we appreciate the interest of the Working Group in data privacy legislation, we are seriously concerned that broad federal preemption would undo years of progress on this issue at the state level and hamstring states' ability to act to protect their citizens by responding to emerging threats and addressing inadvertent weaknesses in any new privacy law. Unless it is extraordinarily strong and futureproof, passing a federal law that broadly prohibits the states from enacting their own laws on data privacy would overall be a substantial net loss for consumers, and would play into the hands of the biggest technology companies like Facebook and Google. For this reason, Consumer Reports opposed the American Privacy Rights Act last year, arguing it would cement an imperfect legal privacy standard in place while depriving states of the ability to take action as they see fit to address the needs of their citizens.[2]

As the Working Group discusses how best to safeguard Americans' personal data, we urge that the principle of *data minimization* be the fundamental framework for any legislation's protections. Under data minimization, companies are limited in processing personal data to what

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

[2] Justin Brookman, *Unclear Protections in the American Privacy Rights Act Not Worth Broad Preemption*, Tech Policy Press, (Apr. 11, 2024), https://www.techpolicy.press/unclear-protections-in-the-american-privacy-rights-act-not-worth-broad-preemption/.

is necessary to fulfill a consumer's request for goods and services (with some limited exceptions). Consumers can take heart that their personal information is protected by default, and do not have to navigate a consent barrage of consent screens or opt-out processes. For many years, Consumer Reports has called on lawmakers to make data minimization the organizing principle of any privacy regulation.[3]

Finally, we stress the need for robust enforcement of any privacy law, as a law enacted without a mechanism for reliable enforcement and consequences for wrongdoers is a law in name only. Over the years, the Federal Trade Commission has been woefully under-resourced and today lacks the legal ability to obtain monetary penalties — or even refunds for defrauded consumers — in most of its cases. The FTC would need reform and dramatically more resources in order to serve as the primary enforcer of a new data privacy law. Furthermore, some capacity for private enforcement of a privacy law should allow for individuals to take action to protect their own privacy interests without having to wait for the government to act.

Below we answer some of the Working Group's specific questions (in italics):

III. Existing Privacy Frameworks & Protections

Since 2016, U.S. trading partners and a growing number of states have enacted comprehensive data privacy and security laws to govern the collection, processing, and transfer of personal information.

A. Please provide any insights learned from existing comprehensive data privacy and security laws that may be relevant to the working group's efforts, including these frameworks' efficacy at protecting consumers and impacts on both data-driven innovation and small businesses.

C. Given the proliferation of state requirements, what is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?

Given the difficulty in getting privacy legislation right, we strongly urge the Committee to adopt the narrowest scope of preemption to invalidate state legislation only to the extent that it directly conflicts with federal law — that is, a federal bill should preempt state legislation only when complying with the state law would result in a violation of the federal law. In theory, a very

[3] Consumer Reports and the Electronic Privacy Information Center, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, Consumer Reports, (Jan. 26, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf; *Model State Privacy Act*, Consumer Reports, (Feb. 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

strong law that meaningfully constrains unwanted data processing could be worth the very high cost of state preemption. However, practice has shown that it is very difficult in practice to enact legislation that is effective in doing so. To date, Congress has failed to enact *any* comprehensive privacy legislation despite numerous legislative efforts dating back to the 1990s.[4] If Congress is actually able to enact a federal privacy law this year or next, it is doubtful it will have the institutional capacity to revisit the law in a timely fashion and make revisions in response to how the law has been implemented in practice. If a law is passed, consumers cannot wait another thirty years before legal privacy protections are reevaluated and updated.

Such a monolithic and static approach has limited Europe's effectiveness in protecting personal privacy. In 2016, Europe passed the General Data Protection Regulation as an effort to strengthen privacy protections for its citizens. However, because of vagueness in key provisions and sporadic enforcement, the GDPR has not been successful in meaningfully reining in the excesses of Big Tech companies. Instead, Europeans are inundated with constant cookie consent screens which have proven to be a tedious and ineffective way to address concerns about online tracking. Efforts to update GDPR and related legislation such as the ePrivacy Directive have stalled.[5]

Where Congress has been ineffective, the states have been the leaders on privacy protection in recent years, with nineteen state comprehensive laws being enacted since 2018.[6] These laws have evolved over time in response to implementation concerns and criticisms from industry and consumers. Early on, states moved away from the California Consumer Privacy Act's unwieldy structure in favor of a more streamlined approach such as in the Connecticut Data Privacy Act. States over time have added on new protections, such as heightened protections for sensitive data, or universal opt out tools[7] in response to criticism about the difficulty in exercising privacy rights.[8] Recently Maryland passed the strongest comprehensive state privacy law, incorporating robust data minimization requirements for data collection —

---

[4] Consumer Internet Privacy Protection Act of 1997, H.R. 98, (introduced Jan. 7, 1997), Electronic Privacy Information Center, https://archive.epic.org/privacy/internet/hr_98.html.

[5] Hunton Andrews Kurth, *European Commission Withdraws ePrivacy Regulation and AI Liability Directive Proposals*, The National Law Review, (Feb. 14, 2025), https://natlawreview.com/article/european-commission-withdraws-eprivacy-regulation-and-ai-liability-directive

[6] *US State Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[7] Allison Schiff, *If You're A Publisher And You Don't Know What A UOOM Is, Then Read This*, AdExchanger, (Jan. 27, 2025), https://www.adexchanger.com/data-privacy-roundup/if-youre-a-publisher-and-you-dont-know-what-a-uoom-is-then-read-this/ (noting 12 of the 19 states to have passed privacy legislation mandate compliance with universal opt-out mechanisms); *Global Privacy Control — Take Control of Your Privacy*, Global Privacy Control, https://globalprivacycontrol.org/.

[8] Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, Consumer Reports, (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf.

meaning companies can only collect the data that is reasonably necessary to deliver a good or service requested by a consumer. Several states are currently considering similar protections. For more on data minimization requirements, *see infra* Responses to Questions II.A-B.

Importantly, while state bills have generally gotten stronger as legislatures adapt language based on other states' experiences, the states that have already enacted legislation have also shown the capacity to go back and revise their own laws to update and strengthen protections. California, which passed the first comprehensive privacy statute in 2018 enacted a comprehensive set of reforms to the law with the California Privacy Rights Act of 2020 and has since added on additional protections such as the DELETE Act, giving consumers the ability to delete data broker records *en masse*. Connecticut, whose legislation has served as a model for several other states, has already amended their law once to add heightened protections for health and minors' data, and is currently considering a number of additional reforms to its law in response to criticisms raised by the Connecticut Attorney General and others.[9] The Oregon legislature is also debating a bill to expand their data privacy law to add, *inter alia*, a prohibition on selling the sensitive data of consumers.

Finally, complying with marginally different state privacy laws has proved to be workable in practice. For years, middleware vendors such as OneTrust and WireWheel have offered easy-to-use portals that allow companies to set different data collection and sharing practices for their websites for different jurisdictions.[10] And of course, the easiest way to avoid enforcement actions is to limit data sharing to only what is needed to perform the services requested by a consumer — state enforcement actions have largely focused on companies that share consumers' personal information with data brokers and Big Tech companies without consumers' understanding let alone permission.[11]

---

[9] *Attorney General Tong Releases Report on Connecticut Data Privacy Act*, The Office of the Attorney General William Tong, (Feb. 1, 2024), https://portal.ct.gov/ag/press-releases/2024-press-releases/attorney-general-tong-releases-report-on-connecticut-data-privacy-act.

[10] @GlobPrivCtrl, X.com, (Oct. 20, 2021), https://x.com/globalprivctrl/status/1450897561158668290.

[11] *E.g.*, *Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies*, Ken Paxton Attorney General of Texas, (Jan. 13, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45; *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*, State of California Department of Justice, (Aug. 22, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

II. Personal Information, Transparency, and Consumer Rights

A federal comprehensive data privacy and security law should apply to personally identifiable information and provide consumers with clear disclosures and rights to their personal information.

B. What disclosures should consumers be provided with regard to the collection, processing, and transfer of their personal information and sensitive personal information?

C. Please identify consumer protections that should be included in a comprehensive data privacy and security law. What considerations are relevant to how consumers enforce these protections and how businesses comply with related requirements?

Setting aside the question of preemption, we urge the Committee to base any proposed legislation upon the principle of *data minimization* to best safeguard consumers' personal information without putting undue burden on them to figure out for themselves how to do so.

Arguably the most important element of any privacy legislation is how to constrain — or to empower consumers to constrain — *secondary use* of their information, including the transfer and use of that data for advertising. Primary uses of data — processing that is necessary to provide the functionality requested by consumers — are typically understandable and noncontroversial. For example, a company may collect a person's mailing address to send them a product they ordered or to process a credit card transaction. On the other hand, secondary use of data is often not well understood, and the benefits often do not accrue directly to consumers — indeed, in many cases, the uses seem downright adversarial or antithetical to people's interests, only serving the interests of companies. Most of the privacy controversy in recent years and motivation for regulation has centered around businesses' disclosure of personal data to data brokers and for online advertising.

For years, the Federal Trade Commission embraced a policy of "notice-and-choice" — companies would publish privacy policies outlining their data processing activities, and consumers would be deemed to have chosen to accept those practices as a condition of using the site. In practice, however, few consumers actually read privacy policies, and when they do, the policies typically include limited practical information. As a practical matter, notice and choice delivers neither notice nor choice. Few would argue that consumers are better off under this regime.

Balancing user autonomy with hard-and-fast rules for secondary processing can be quite challenging in practice. Legislative proposals to limit secondary uses of personal data historically

applied either "opt-in" or "opt-out" frameworks — a requirement that companies must either ask for affirmative permission for secondary processing, or that they must give consumers the ability to turn off secondary processing. Both models can be flawed in practice: opt-in models can overwhelm consumers with constant requests for permission, as many websites have done in response to European privacy law. Companies may use dark patterns to coax consumers already weary so they click "OK" to cede permission for any and all uses. Meanwhile opt-out regimes such as are seen in state privacy laws are both difficult to use and wildly impractical if one is to protect oneself in any meaningful way, if consumers have to manually opt out of secondary use for every website, app, or business they interact with, which can amount to thousands of organizations. As a result of both approaches, consumers are forced to take too many steps to safeguard their data.

A better model would either constrain data processing to conform to expected privacy norms by default. This is what data minimization is designed to do. Under a data minimization standard, companies can only process data as is reasonably necessary to fulfill a consumer's request. This model does not rely upon consent or opt-outs — instead a company performs the reasonably expected data processing without burdening the consumer. The company should document its data practices in a privacy policy, but it should not be expected that consumers will normally read these policies — instead, they function more like financial filings that are interpreted by regulators and sophisticated investors. If some necessary data processing is potentially unexpected or especially sensitive, the company should make sure the consumer understands through heightened notice where the consumer would be likely to notice it.

Of course, such a model should specify operational exceptions that are not necessarily directly necessary for fulfillment, but which are reasonably necessary to maintain a business — purposes such as security and fraud prevention, analytics, accounting, and product improvement. These exceptions should be narrowly and carefully crafted to avoid creating inadvertent loopholes that vitiate the intent to constrain unnecessary data collection and sharing. For example, monetization of personal data through data sales should never be construed as an operational exception to the data minimization standard.

Finally, it is important to stress that, narrow operational purposes aside, data processing should be limited to the purposes of *the consumer*, and not just any purposes envisioned by the company. Some purported data minimization frameworks only require companies to list all putative purposes within a privacy policy, and restrict companies only from additional data processing beyond that. Such frameworks do little if nothing to actually protect privacy or constrain data processing, as companies simply adopt the same broad reservations of rights in dense, legalese privacy policies that few consumers read as they did under the old notice-and-choice framework. Instead, a true data minimization framework should limit data

processing to what is needed to fulfill specific consumer requests for goods and services, with narrowly crafted operational exceptions that are necessary for businesses to operate.

VI. Accountability & Enforcement

Accountability and enforcement are cornerstones of a data privacy and security regime that protects consumers, promotes compliance, and enables data-driven innovation.

A. Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.

B. What expertise, legal authorities, and resources are available—or should be made available—to the Federal Trade Commission and state Attorneys General for enforcing such a law?

For thirty years, the Federal Trade Commission has been the lead federal agency on consumer privacy, and it has brought a number of important cases to challenge behaviors that threaten personal privacy and security. However, the FTC has been severely underfunded for decades and currently lacks the capacity to enforce a new privacy law on its own. Currently, the FTC only has 1292 FTEs total to pursue both its competition and consumer protection missions.[12] This number has been roughly flat over the past fifteen years, and actually represents a decrease from 1746 FTEs in 1979. Put another way, the economy is three times larger than it was in 1979 while the FTC's capacity has decreased 26 percent. And this figure does not reflect recent or future cuts from the Department of Governmental Efficiency which may cripple the FTC's capacity to protect consumers even further.

Moreover, the FTC currently lacks the ability to obtain monetary penalties or even restitution of stolen funds or ill-gotten gains in many of its cases. Since the Supreme Court's decision in *AMG Capital Management, LLC v. Federal Trade Commission* three years ago,[13] Congress has tried and failed to restore to the FTC the ability to obtain refunds on behalf of consumers or to obtain other equitable relief to ensure that wrongdoers do not retain the benefits of their fraudulent practices. Given Congress's inability to pass even this narrow fix to allow the FTC to get refunds on behalf of defrauded consumers, it would be unwise to vest all enforcement authority with a fundamentally hamstrung agency.

---

[12] FTC Appropriation and Full-Time Equivalent (FTE) History, Federal Trade Commission, https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation.

[13] 593 U.S. 67 (2021).

State Attorney Generals offer enforcement capacity as well, though to date only a handful of cases have been brought under the nineteen comprehensive privacy laws that have passed. The majority of states that have passed such privacy laws have not brought any enforcement actions *at all*. And this is not for a lack of ready targets — Consumer Reports has put out a number of reports demonstrating noncompliance with state privacy laws, including a report from last week showing that many companies were showing targeted ads despite receiving legally binding universal opt-out signals.[14] In fact, like the FTC, most state Attorney General offices are underresourced and do not have the capacity to bring enough actions to meaningfully deter illegal behavior.

Any privacy law thus should provide for some degree of private enforcement, to empower individuals to take action to safeguard their own privacy without waiting for a government agency to intervene. Industry has raised concerns about costs and bad faith strike suits. However, a private right of action is not a monolithic concept, and several commentators have tried to find a reasonable middle ground to allow for good faith actions against wrongdoers without offering perverse incentives to actors simply looking to extract a legal settlement based on a questionable factual premise.[15]

Thank you very much for your consideration of these responses to the Working Group's questions. We are happy to engage further with members of the Committee as they explore data privacy issues; please contact Justin Brookman at justin.brookman@consumer.org if you have any additional follow-up questions or if there is anything else we could do to assist the Committee.

Sincerely,

Justin Brookman
Director, Technology Policy
Consumer Reports

---

[14] Matt Schwartz *et al.*, *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws*, Consumer Reports, (Apr. 1, 2025), https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf; Maggie Oates *et al.*, *Companies Continue to Share Health Data Despite New Privacy Laws*, Consumer Reports, (Jan. 16, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf.

[15] Paula Bruening, *How to end the deadlock on the private right of action*, IAPP, (Jan. 20, 2022), https://iapp.org/news/a/how-to-end-the-deadlock-on-the-private-right-of-action; Joseph Jerome, *Private right of action shouldn't be a yes-no proposition in federal US privacy legislation*, IAPP, (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/.