CENTER FOR DEMOCRACY & TECHNOLOGY

April 7, 2025

To: House Energy & Commerce Committee Privacy Working Group
2125 Rayburn House Office Building
Washington, DC 20515

Re: Request for Information on Federal Comprehensive Data Privacy and Security Framework

I. Introduction

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the House Energy & Commerce Committee Privacy Working Group's request for information (RFI) regarding a federal comprehensive privacy and security framework. CDT is a nonpartisan, nonprofit organization that works to advance civil rights and civil liberties in the digital age.

We appreciate the opportunity to comment and the committee's desire to gather more information from stakeholders about their privacy viewpoints and evidence of data practices and their harms. A significant amount of work has been done in the past several years to achieve bipartisan consensus on key elements of a federal privacy framework, and we urge the Working Group to build on this consensus. Our comments focus on many of those areas of consensus and offer further thoughts on other issues.

Any effective federal privacy law must place limits on companies' collection, use, processing, and sharing of data to protect individuals from harm. These harms include fraud and other economic injury, discrimination, reputational harm, harassment, and government surveillance that circumvents the Fourth Amendment and other legal protections. Because many of these risks increasingly arise from the use of artificial intelligence (AI) such as in automated decision-making systems, an effective 21st century privacy framework should account for AI. Protecting privacy will bolster consumer trust in our increasingly data-centric economy and thereby enable greater innovation.[1]

[1] Julie Heng, *Moving Beyond the Regulation/Deregulation Trap*, Center for Strategic & International Studies (Feb. 20, 2025), https://www.csis.org/blogs/perspectives-innovation/moving-beyond-regulationderegulation-trap; Jaime Leverton, *Well-Done Regulation Can Spur Innovation: How Companies Can Get Involved*, Forbes (Mar. 27, 2023), https://www.forbes.com/councils/forbesbusinesscouncil/2023/03/27/well-done-regulation-can-spur-innovation-how-companies-can-get-involved/; Organisation for Economic Co-operation and Development, *Regulation and Innovation*, https://www.oecd.org/en/topics/better-regulation-and-innovation.html.

CENTER FOR DEMOCRACY & TECHNOLOGY

II. Key consumer protection requirements

The Privacy Working Group correctly recognizes that a privacy framework should "provide consumers with clear disclosures and rights to their personal information," and that "accountability and enforcement are cornerstones" of a framework that protects consumers. Such a framework is critical as the data ecosystem expands and companies incorporate more personal data into AI systems. Companies that deploy these systems can select which personal data the systems will analyze to produce outputs that influence decisions affecting people's access to employment, housing, financial services, and other critical opportunities and services. In addition, AI systems are trained on massive datasets, which incentivizes companies to build the largest possible datasets filled with data from all available sources, including sources with uncertain or nonexistent quality-assurance practices – for example, data collected through web scraping or from third parties.

To achieve the goals described in the RFI, a privacy framework should prioritize several important elements:

A. Data minimization and purpose limitations should be the foundation of a privacy framework.

A privacy framework should not place the burden of privacy protection on consumers through a notice-and-choice regime, but on the entities that most benefit from their data practices by centering on data minimization and purpose limitations:[2]

- Data minimization: companies should collect only the data they need to provide a product or service.
- Purpose limitation: companies should be subject to limits on the types of purposes for which they can collect, process, and transfer data.

Data minimization and purpose limitations help prevent privacy harms at the outset, because data a company does not have cannot lead to downstream harm through misuse, unauthorized access or disclosure, or some other action that causes harm. Data minimization requirements have bipartisan support from Americans: a recent Consumer Reports survey found that

[2] For more, see Eric Null, *States Are Letting Us Down on Privacy*, Center for Democracy & Technology (Jan. 28, 2024), https://cdt.org/insights/states-are-letting-us-down-on-privacy/.

seventy-two percent of Republicans and seventy-nine percent of Democrats "support a law that limits companies to using only the data they need to provide their service."[3] Reining in data collection, use, and sharing would limit companies' ability to violate consumer protection laws and civil rights laws through digital practices.

Both the American Data Privacy Protection Act (ADPPA) and the American Privacy Rights Act (APRA), which were the subject of House Energy & Commerce hearings and votes, contained data minimization provisions and purpose limitations. Under ADPPA, a company's collection, processing, retention, and sharing of non-sensitive personal information was restricted only to information that was reasonably necessary and proportionate to provide the service the consumer was specifically requesting. Sensitive personal information could be collected, processed, and retained only to the extent strictly necessary to provide the requested service. Sensitive personal data could not be transferred without affirmative express consent. Under APRA, data could be collected, processed, and transferred only to the extent necessary, proportionate, and limited to the product or service the consumer was requesting.

Any additional permissible purposes should be clear and unambiguous. Allowable purposes for using collected data could include, for example, complying with existing legal obligations, protecting data security, effectuating product recalls, conducting legally compliant research in the public interest, or detecting or preventing safety threats. When a company collects, uses, or shares people's personal data for these allowable purposes, it should be only to the extent necessary to fulfill these purposes.

Industry often argues that robust data protections will stifle innovation and inhibit the development of new technologies that people do not yet know they want, because newer technologies can require greater volumes of data to perform as promised. However, an exception for product development and marketing could easily swallow the rule, as essentially any data could be justified as "product development." To the extent such an exception is necessary, it should be carefully circumscribed, such as for the development of the product or service specifically being requested by the consumer.

[3] Scott Medintz, *Americans Want Much More Online Privacy Protection Than They're Getting*, Consumer Reports (Nov. 20, 2024), https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306/.

B. Clear, user-friendly disclosures should be just one part of a broader set of protections.

Disclosures are a necessary, but not sufficient, aspect of a privacy framework. The notice-and-consent approach to consumer privacy fails to protect privacy – instead, it simply overwhelms people. Users cannot be expected to review privacy policies for every website, app, and connected device they use. We know they do not. In 2023, the Pew Research Center reported that fifty-six percent of American adults say they agree to privacy policies without reading them, compared to eighteen percent who say they rarely or never agree without reading.[4] Further, sixty-one percent of adults consider privacy policies to be an ineffective way for companies to explain data practices, and sixty-nine percent consider privacy policies to be just something to "get past."[5] Researchers have identified several factors contributing to consent fatigue, including information overload, people's sense of futility and lack of control over privacy risks, and their underestimation of the risks of providing information.[6] Further, a 2008 study estimated that if people were to read the privacy policies of all websites they visit, they would spend 244 hours a year, or an average of forty minutes a day, reading privacy policies.[7] Ten years later, privacy policies were found to have doubled in length and have become less readable, with many policies also linking to additional policies for users to review.[8]

The public is looking to policymakers to move us beyond notice-and-consent and push companies toward proactive data protection measures. The vast majority of respondents to a December 2024 Deloitte survey agreed that privacy policies do not help them control their data – ninety percent stated they want technology companies to do more to protect their data, and eighty-four percent want the government to do more to regulate how companies collect and use consumer data.[9]

---

[4] Colleen McClain et al, *How Americans View Data Privacy*, Pew Research Center (2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[5] *Id.*
[6] Wenjun Wang et al, *An Exploration of the Influencing Factors of Privacy Fatigue Among Mobile Social Media Users From the Configuration Perspective*, Scientific Reports (2025), https://www.nature.com/articles/s41598-024-84646-z.
[7] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society 540, 560 (2008), https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2013/02/Cranor_Formatted_Final1.pdf.
[8] Ryan Amos et al, *Privacy Policies Over Time: Curation and Analysis of a Million-Document Dataset*, In Proceedings of the Web Conference (2021), https://arxiv.org/pdf/2008.09159.
[9] Jana Arbanas et al, *Earning trust as gen AI takes hold: 2024 Connected Consumer Survey*, Deloitte (2024), https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html.

Further, mere disclosures of data practices have been gamed by companies. Companies have obscured their data practices through dense, confusing privacy policies, or notices with deceptive user interfaces and design elements, called dark patterns, that nudge and encourage people to share more data than they would otherwise want. These tactics have enabled some companies to impute consent from people's use of their products without taking steps to help people understand what is happening with their data. Meaningful transparency also would involve easy-to-understand disclosures in formats that are easy to navigate and accessible for disabled people.

The lack of transparency poses additional concerns when personal data is used in automated decision-making systems. Without knowing how these systems analyze personal data and how the systems' outputs influence decision outcomes, people are ill-equipped to successfully challenge highly consequential decisions such as whether they can get a loan or housing even if they are made erroneously due to incorrect data. People are at an additional disadvantage when sources of training data are not disclosed, making it difficult to know where to direct efforts to try to correct or delete one's own data.

C. Explicit civil rights safeguards should be included to curb discriminatory data-driven decisions.

Privacy rights are civil rights. A privacy framework needs to protect civil rights because data has been used to take discriminatory actions against individuals based on protected characteristics. For example, publicly available records combined with financial and other personal data are factored into decisions about eligibility for rental housing and insurance coverage and premiums – without additional context, some of this data, such as court records and prior addresses, would tend to disqualify people based on protected characteristics.[10] A privacy framework should explicitly affirm that it is unlawful for companies and their service providers to collect, process, or transfer personal information in a manner that discriminates against individuals based on protected characteristics and makes equal opportunity and enjoyment of goods and

[10] Sara Sternberg Greene et al, *Getting to Home: Understanding the Collateral Consequences of Negative Records in the Rental Housing Market*, 74 Duke Law Journal 269 (2024), https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=4213&context=dlj; Marshall Allen, *Health Insurers are Vacuuming Up Details About You – And It Could Raise Your Rates*, ProPublica (Jul. 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

services unavailable.[11] Companies should have to affirmatively take steps to prevent such discriminatory decisions, such as by using alternative data, using alternative methods for making decisions, or requiring human review. To ensure their systems can be tested for discrimination, companies should also be allowed to collect demographic data for the express and limited purpose of ensuring their systems do not discriminate and to ensure that all consumers can trust these systems.

Companies should proactively assess and mitigate discrimination risks in any algorithmic system that makes a decision or assists human decision-making using personal information to advertise or to determine access to or terms of housing, employment, healthcare, insurance, or credit opportunities. This process should occur before an algorithmic system is deployed and on an ongoing basis after deployment. After deployment, companies should regularly conduct algorithmic impact assessments that describe the system's methodologies, intended purpose, proposed and actual uses, and actual data inputs and outputs. These assessments should also describe if the system is fit-for-purpose, and the steps taken to mitigate and prevent discrimination risks.

D. The use and sharing of personal data for targeted advertising should be restricted.

Protecting privacy requires grappling with the online advertising industry's data practices. A federal privacy framework should center the interests of three stakeholder groups: ordinary internet users, online publishers, and advertisers themselves. Industry groups dominated by ad-tech intermediaries (including small, medium, and large businesses) falsely assert that any effort to regulate the collection and use of data for ad targeting will inevitably cause web publishers' revenues to crater and kill the open internet. This false dichotomy should be rejected: online advertising can take several forms, many of which are compatible with robust privacy protections and can economically support the creation and availability of content.

A privacy framework should distinguish between types of advertising along two axes: how the ads are targeted, and the provenance of the data used for targeting.

[11] In many contexts, existing civil rights statutes apply to companies whose use of personal data results in discrimination, but enforcement is often difficult for two main reasons. First, both the public and regulators lack visibility into the nexus between a company's data practices and the discriminatory results. Second, the exchange of personal data and the use of third-party algorithmic systems allows decision-makers and their service providers or other affiliates to each deflect responsibility for civil rights violations stemming from automated decision-making.

On targeting, the framework should distinguish between behavioral and contextual advertising. Contextual targeting is based on the immediate content of the webpage, app, or online service the person is viewing, or the search query the person submits, and approximate geolocation. Such advertisements are displayed only in proximity to the content or search results the person is viewing.[12] In contrast, behavioral targeting seeks to reach specific individuals or groups of individuals based on their demographic and behavioral characteristics, as inferred from data from any source. It thus incentivises companies to indiscriminately collect as much data as possible, on the theory that "personalized" advertising delivers greater value to advertisers and consumers. While this claim is vigorously contested, not least because of data quality issues, it nonetheless spurs demand for personal data sales, giving rise to the data broker industry and incentivizing even more data collection. Behavioral advertising can cause people to receive unwanted and even distressing advertisements because advertisers are targeting vulnerable users,[13] or it can prevent people from learning about services, products, or opportunities they do want to pursue because advertisers exclude them from the target audience.[14]

On the provenance of data, the framework should distinguish between first- and third- party advertising, and cross-contextual behavioral advertising. First-party behavioral targeting is based on a user's activity on the website (or app) they are viewing, and third-party behavioral targeting is based on data of a single third-party advertiser, such as retargeting. Cross-contextual behavioral targeting is based on a user's browsing activity over time and across websites (using cookies/device fingerprinting/etc.), and/or digital dossiers that ad-tech vendors or data brokers compile about users on the basis of cross-site tracking data.

Contextual targeting and first-party targeting generally do not undermine people's privacy and should be allowed. A privacy law should, however, provide protection from the invasive data practices that undergird other forms of targeted advertising. For example, individuals should be able to opt out of third-party targeting, and cross-contextual behavioral targeting and targeting on the basis of sensitive data should be prohibited.

---

[12] Nathalie Maréchal and Nick Doty, Center for Democracy & Technology, Defining Contextual Advertising (2024), https://cdt.org/insights/brief-defining-contextual-advertising/.

[13] Liza Gak, Seyi Olojo, & Niloufar Salehi, *The Distressing Ads That Persist: Uncovering The Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating*, 1 Assoc. For Computing Mach. 9 (April 2022), https://arxiv.org/pdf/2204.03200.pdf; Sauvik Das and Yuxi Wu, *How Online Behavioral Advertising Harms People*, Center for Democracy & Technology (Dec. 13, 2023), https://cdt.org/insights/how-online-behavioral-advertising-harms-people/.

[14] Clare Duffy and Carlotta Dotto, *People Are Missing Out on Job Opportunities on Facebook Because of Gender, Research Suggests*, CNN (Jun. 12, 2023), https://edition.cnn.com/2023/06/12/tech/facebook-job-ads-gender-discrimination-asequals-intl-cmd/index.html.

E. Universal opt-out mechanisms should be widely available, and opt-out preference signals should be honored.

In addition to opting out of companies' use of personal information for third-party targeted advertising, people should also have the right to opt out of the sharing of personal data for other purposes. As APRA did, a privacy framework should require all covered entities to provide people with a clear, easy-to-use means of opting out, and to abide by that opt-out request.[15] However, signaling an opt-out for every individual website or app can be burdensome. To ease that burden, the framework should require browsers and operating systems to provide a universal opt-out mechanism, such as the Global Privacy Control setting currently provided by certain browsers,[16] that communicates a signal to all websites and apps a person's request to opt out of the collection, processing, or transfer of their data. This mechanism should be designed to be effective for all users, ensuring language access as well as usability for people with disabilities.

III. Scope of key definitions

A. Definitions for "personal information" and "sensitive personal information" should draw from previous established consensus.

ADPPA and APRA reflected a bipartisan consensus on the scope of covered data that should be instructive. Personal information should be defined as information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or to a device that identifies or is linked or reasonably linkable to an individual.

Certain limited exclusions may be appropriate, including:

- De-identified information: information that does not identify and is not linked or reasonably linkable to an individual or to a device that is linked or reasonably linkable to the individual.

[15] Matt Schwartz at al, *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws*, Consumer Reports (2025), https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf.

[16] Nick Doty and Cami Goray, *It's Time to Standardize the Global Privacy Control*, Center for Democracy & Technology (Dec. 13, 2023), https://cdt.org/insights/its-time-to-standardize-the-global-privacy-control/.

- Publicly available information: information that a covered entity has a reasonable basis to believe has been lawfully made available to the general public.

Personal information should exclude de-identified information only if covered entities are required to take reasonable physical, administrative, and technical measures to prevent the data from being re-identified by a covered entity or any other party with whom that entity shares the information. Inferences from publicly available information that do not reveal sensitive personal data can be exempted from the substantive privacy protections.

A privacy framework should also protect the types of sensitive personal information enumerated in ADPPA and APRA. A similar definition of "sensitive personal information" in those bills was adopted in the Protecting Americans' Data from Foreign Adversaries Act.[17]

B. The scope of "covered entities" should be broad, as privacy harms can come from a variety of companies of all shapes and sizes.

When defining a covered entity, a privacy framework should apply broadly to every company that engages in collecting, processing, retaining, or transferring personal information, unless there is a compelling reason to exempt it. Covered entities should include airlines and banks, which have long been exempt from general privacy laws. Small businesses are also capable of causing serious privacy harms – consider Cambridge Analytica, for example – and should therefore be covered, perhaps with exemptions from particular requirements. A clear federal privacy standard would help small businesses compete while preserving their customers' trust.[18] In general, every business should bear responsibility for data minimization, purpose limitations, restrictions on selling data, and deletion or de-identification requirements.

Covered entities should also include data brokers, which derive their revenue from sharing or selling personal information that they did not directly collect from the person linked to that information. A mandatory data broker registry and a universal mechanism that allows people to send data deletion requests to all data brokers should also be included in a privacy framework.

Developers and deployers of AI/algorithmic systems should each have responsibilities under the framework as well. For example, both types of entities should assess risks at the stages of the

[17] 15 U.S.C. §9901(c)(7).
[18] ACT | The App Association, *Protecting Consumer Privacy, Growing Small Business* (2020), https://actonline.org/wp-content/uploads/Privacy_2020.pdf.

system's life cycle in which they are involved. Developers should be responsible for algorithm design evaluations, and deployers should be responsible for impact assessment requirements. Developers should provide deployers with all the information about developers' risk evaluations that is necessary for deployers to ensure their impact assessments properly examine all risks.

IV. Enforcement

Laws are only as meaningful as their enforcement, particularly when covered entities are numerous, compliance is highly technical, and non-compliance may be difficult to detect.

Federal privacy enforcement should be multi-pronged, leveraging federal and state agencies, state attorneys general or other privacy enforcers, and a private right of action. Agencies have the established subject-matter expertise and regulatory experience to enforce their authorizing statutes. The Federal Trade Commission (FTC) would be especially well-positioned to enforce a privacy law, as an independent agency with a multi-member bipartisan structure that ensures agency actions are well-informed.[19] The FTC already takes on a significant load holding companies operating nationally accountable, and increased investment in the agency would bolster its enforcement of a new privacy law.[20] State agencies and attorneys general have already begun enforcing their own privacy laws, and can supplement the FTC's role given their expertise in the issues that most impact their constituents. Government enforcers, however, have limited capacity and cannot police every company; therefore, as with many other consumer protection laws, individuals should also be able to pursue private claims so they can

[19] FTC Chair Ferguson recently expressed agreement about the importance of the FTC's multi-member bipartisan structure. Joe Weisenthal and Tracy Alloway, *FTC Chief Andrew Ferguson on the Trump Vision for Antitrust*, Bloomberg Odd Lots (Mar. 17, 2025), https://omny.fm/shows/odd-lots/ftc-chief-andrew-ferguson-on-the-trump-vision-for ("There's also I think some benefits in certain circumstances to having multi-member agencies with people from both parties. I mean, look, if you have an agency that is exceeding the law, abusing the companies that it purports to regulate, it's helpful for markets, for courts, for litigants, for government transparency to have people in the other party pointing this out and saying it in dissents. Like you know, I wrote four hundred plus pages of dissents during my time as a Minority commissioner. I think that that adds value.").

[20] *The World Wide Web: Examining Harms Online*: *Hearing Before House Subcommittee on Commerce, Manufacturing, and Trade*, 119th Cong. (testimony of FTC Commissioner Rebecca Slaughter), https://d1dth6e84htgma.cloudfront.net/Testimony_Rebecca_Kelly_Slaughter_b78a97396e.pdf; *CDT CEO Alexandra Givens Testimony Before House Energy & Commerce Hearing on "Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy"*, Center for Democracy & Technology (Mar. 1, 2023), https://cdt.org/insights/cdt-ceo-alexandra-givens-testimony-before-house-energy-commerce-hearing-on-promoting-u-s-innovation-and-individual-liberty-through-a-national-standard-for-data-privacy/.

be made whole in the event that government agencies do not pursue their claims. There is significant bipartisan support for a private right of action.[21]

V. Interaction with state privacy laws

In the absence of a federal privacy law, states, as the laboratories of democracy, have begun passing their own privacy laws, ranging from comprehensive laws to data broker limits or requirements for automated decision-making systems. For instance, California has been enforcing, and pursuing new implementing regulations for, its privacy law, and Maryland has passed a strong law that emphasizes data minimization. Other states, however, have taken an approach that merely blesses the notice-and-consent regime that has blossomed over the past three decades, with "data minimization" protections that allow any data collection and processing for any purpose the company discloses – essentially, these bills merely require longer privacy policies and *more* consent mechanisms, leading to consent fatigue and confusion.[22]

States have been active in privacy in part because of the void left at the federal level. In general, states were not passing privacy laws before 2019. If Congress passes meaningful privacy legislation that truly protects consumers, it is likely that states would feel less need to pass comprehensive privacy laws. Nevertheless, states would still have an important role to play, including in areas that overlap with privacy in which they have traditionally had a significant role, such as addressing unfair and deceptive practices and civil rights protections. Thus, even if any preemption beyond conflict preemption (which already would apply by virtue of the Supremacy Clause) were appropriate – and it would not be if the federal law did not provide strong substantive privacy protections such as those described above – it should leave in place the ability of states to legislate in specific areas, much as APRA and ADPPA would have done.

---

[21] For example, Republican Senator Josh Hawley has signaled support for a private right of action in privacy. Leila Fadel, *Republican Sen. Josh Hawley Discusses His Mission to Hold Big Tech Accountable*, NPR (Feb. 27, 2025), https://www.npr.org/2025/02/27/nx-s1-5302712/senator-josh-hawley-data-privacy-censorship-doge ("I think the fact that they can take our data without our knowledge, they can sell it without our permission, they can market it without our control — all of these are huge problems. We should give every single American the right to go to court and to sue these companies when they violate our property rights, when they take it from us without our consent and without any form of compensation. And also when they harm our children, when our kids are exposed to sexually exploitative material, we ought to be able to go to court and sue these companies. Right now, we can't. And that needs to change.").

[22] Eric Null, *States Are Letting Us Down on Privacy*, Center for Democracy & Technology (Jan. 28, 2024), https://cdt.org/insights/states-are-letting-us-down-on-privacy/.