epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

The Electronic Privacy Information Center (EPIC) appreciates the opportunity to provide feedback to the Privacy Working Group led by the Majority Leadership of the House Committee on Energy and Commerce. Federal privacy legislation must limit the collection and use of Americans' personal data with rules that respect our human right to privacy, limit harmful discrimination and targeting, and support the beneficial evolution of the technologies and systems we rely on in our everyday lives. EPIC has long advocated for strong privacy laws at the federal and state levels and is ready and willing to be a resource to the Privacy Working Group as it seeks to provide comprehensive privacy protections to all Americans.

As Congress considers federal privacy legislation, it should learn from and improve upon existing state laws by strengthening privacy protections. The Virginia/Connecticut "models" and the state laws that follow them do not adequately protect privacy. Many of those laws have been heavily influenced by lobbying groups doing the bidding of Big Tech companies, leading to "privacy" laws that, in fact, do little to protect privacy.[1] In a recent report scoring 19 state privacy laws by EPIC and the U.S. PIRG Education Fund, eight received Fs, and none received an A.[2]

EPIC has been calling on Congress to pass a strong comprehensive privacy law for more than 25 years[3] – but the enactment of a weak law that cements the current status quo into law is worse than passing no law at all. Any federal privacy legislation must reflect the reality that America is in a data privacy crisis and that regulation is badly needed to encourage privacy-protective innovations in technology and ensure privacy, fairness, and security in our online world. EPIC would welcome the opportunity to engage with the working group on ways to craft privacy legislation that meets the moment.

---

[1] *See* 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/; Todd Feathers & Alfred Ng, *Tech Industry Groups Are Watering Down Attempts at Privacy Regulation, One State at a Time*, The Markup (May 26, 2022), https://themarkup.org/privacy/2022/05/26/tech-industry-groups-are-watering-down-attempts-at-privacy-regulation-one-state-at-a-time.

[2] *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better,* EPIC and U.S. PIRG Education Fund (Jan. 2025), https://epic.org/state-of-privacy-2025.

[3] *See e.g. 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 ("the 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.")

I. Roles and Responsibilities

A. How can a federal comprehensive data privacy and security law account for different roles in the digital economy (e.g., controllers, processors, and third parties) in a way that effectively protects consumers?

The most effective way to protect consumers is to ensure that *any entity* handling personal data is obligated to limit the collection and use of that data in line with consumers' expectations. We go into detail on what these rules should look like in our response to Question III(A).

B. What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?

All entities that collect, process, or transfer personal data (including non-profits) should have obligations to protect and secure that data.

C. Should a comprehensive data privacy and security law take into consideration an entity's size, and any accompanying protections, exclusions, or obligations?

EPIC has acknowledged that smaller entities could be properly exempted from some provisions of a comprehensive privacy law to minimize regulatory costs. However, any thresholds for coverage should be based on the amount of data a company collects or processes, not on revenue – many startups might have no revenue but do have the ability to collect mass amounts of personal data.

II. Personal Information, Transparency, and Consumer Rights

A. Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."

We refer the Working Group to the definitions spelled out in the model bill recently released by EPIC and Consumer Reports, the State Data Privacy Act.[4]

[4] EPIC and Consumer Reports, *The State Data Privacy Act*, https://epic.org/documents/the-state-data-privacy-act/.

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

Disclosures alone are simply not a sufficient way to protect consumers' privacy. Despite being the hallmark of the failed "notice and choice" regime, disclosures overwhelm consumers without providing meaningful protection. Consumers cannot reasonably be expected to read long, technical privacy policies for every website or app with which they interact, especially because these disclosures do not give consumers any real choices about their privacy—the all-or-nothing decision to either accept the terms of a privacy policy or to simply not access the service is not a meaningful choice.

Instead of inundating consumers with even more disclosures, a federal privacy law should include data minimization principles that better align businesses' data practices with what consumers expect. Please see our response to Question III(A) for more detail.

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?

The most important element that must be included in a federal privacy law is a strong data minimization framework. See our response to Question III(A) for details about what a strong data minimization standard looks like.

Consumers should be granted all the basic rights that are in state privacy laws—the right to access, correct, and delete personal information; the right to opt out of the processing of the consumer's personal data for targeted advertising or profiling and to opt out of the sale of the consumer's personal data; and the right to obtain a list of third parties to whom a controller has disclosed the consumer's personal data. These consumer rights must also be easy for consumers to exercise; privacy rights that are too onerous for consumers to use do nothing to protect their privacy. To this end, a federal privacy law must include provisions granting consumers the right to use an authorized agent to exercise their privacy rights on their behalf and requiring that companies recognize a universal opt-out mechanism. These mechanisms, which businesses are already required to comply with under the majority of state privacy laws, allow consumers to more easily exercise their privacy rights.

Any federal privacy law should also protect consumers from data-driven discrimination – covered entities must be prohibited from using personal data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability.

Consumers should also be able to use their privacy rights to control their personal data without the threat of discrimination. Controllers should be prohibited from charging consumers a different price or offering them a different level or quality of product or service because they exercised their privacy rights.

Finally, any proposed privacy legislation should grant rulemaking authority to an expert agency. Rulemaking authority is necessary both because statutory text can only provide a certain amount of clarity and to keep up with the rapid pace of technological development.

D. What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?

Because of its nature, sensitive personal information should be subject to heightened protections. These heightened protections should include both a prohibition on the sale of sensitive personal information and a requirement that any collection, processing, or transferring of sensitive personal information be limited to circumstances where such use is strictly necessary. States have led the way on protecting sensitive data, including through banning the sale of geolocation or other sensitive information,[5] adopting the "strictly necessary" standard for collection and processing of sensitive data,[6] and placing enhanced protections on the personal data of children and minors[7] and on health information.[8]

III. Existing Privacy Frameworks & Protections

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.

EPIC is one of the most active groups in the country working to provide resources and expertise to state legislators as they develop comprehensive privacy laws, and we would be happy to brief the working group on our takeaways from that work.[9] The biggest weakness in most existing state privacy laws is the lack of a meaningful data minimization standard.

---

[5] Md. Code Ann. Com. Law § 14-4607.
[6] Md. Code Ann. Com. Law § 14-4607.
[7] *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.
[8] *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).
[9] *See generally The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, EPIC (Jan. 2025), https://epic.org/state-of-privacy-2025; Caitriona Fitzgerald & Kara Williams, *The State Data Privacy Act: A Proposed Model State Privacy Bill*, EPIC (Sept. 25, 2024), https://epic.org/the-state-data-privacy-act-a-proposed-model-state-privacy-bill/.

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. Unfortunately, this is what state laws — other than California's and Maryland's — currently allow. Most existing state privacy laws only limit collection to what is reasonably necessary for "the purposes for which such data is processed, *as disclosed to the consumer*," meaning businesses can collect data for whatever purposes they want, as long as they state that purpose in their privacy policies.[10] This reinforces the failed status quo of "notice and choice" — businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them. In fact, it incentivizes companies to list as many purposes as possible, and as broadly as possible, to cover every conceivable reason they would ever want to collect your data. And the only "choice" the consumer has is to not use the service at all.

In passing the Maryland Online Data Privacy Act (MODPA) last year, Maryland legislators took inspiration from the data minimization standard in the American Data Privacy and Protection Act and American Privacy Rights Act that were developed through a bipartisan and bicameral process. MODPA goes into effect on October 1, 2025, and requires that companies limit their collection of personal data to what is *reasonably necessary to provide the product or service the consumer requested*. This aligns companies' data practices with what consumers expect.

To meaningfully protect privacy, any federal privacy law must include real data minimization protections that limit the collection and use of personal data to what is necessary to provide the product or service the consumer is asking for.[11] When reviewing any proposal or draft provisions, the working group should consider whether the proposed legislation would require any change in privacy practices other than amendments to a company's privacy policy or terms of service; if it would not, then it is a weak (and mostly pointless) proposal.

Lobbyists representing Big Tech interests will typically fight against a strong data minimization provision by arguing that it would block specific data uses or harm the online ecosystem by blocking advertising. But a strong data minimization standard will not prevent businesses from advertising. Rather, these laws will encourage ad tech providers to innovate on privacy-protective forms of advertising.

EPIC and Consumer Reports recently released the State Data Privacy Act, a proposed redline to the Connecticut Data Privacy Act, which is the model most cited by industry as the law

[10] *See The State of Privacy 2025: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, EPIC and U.S. PIRG Education Fund (Jan. 2025), https://epic.org/wp-content/uploads/2025/01/EPIC-PIRG-State-of-Privacy-2025.pdf.
[11] Caitriona Fitzgerald & Kara Williams, *Data Minimization Is the Key to a Meaningful Privacy Law*, EPIC (May 2024), https://epic.org/data-minimization-is-the-key-to-a-meaningful-privacy-law/.

they would like other states to emulate.[12] We suggested strengthening amendments, largely based on language that has already been passed in at least one state. We included additional definitions and clarifying language on advertising to the data minimization provisions in an effort to respond to concerns voiced by chambers of commerce and retail associations in various states. We suggest that the State Data Privacy Act would be a helpful resource to the Working Group as it considers language for a potential federal privacy law.

B. Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.

Most existing state privacy laws are actually built on a common framework, and the emerging difference is to what degree the laws enshrine a notice and choice regime or actually impose meaningful data minimization standard to protect consumers.

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?

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 Driver's Privacy Protection Act, the 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.

[12] EPIC and Consumer Reports, *The State Data Privacy Act*, https://epic.org/documents/the-state-data-privacy-act/.

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 serve as a deterrent to states to enact additional laws until changes in technology necessitate it.

D. How should a federal comprehensive privacy law account for existing federal and state sectoral laws (e.g., HIPAA, FCRA, GLBA, COPPA)?

Because these laws are years (or decades) old and were often not intended to be privacy laws in the first place, a federal comprehensive privacy law does not need to include exemptions for these laws. In fact, in a report the published this year on the Connecticut Data Privacy Act, the Connecticut Attorney General urged the legislature to amend the law to scale back entity-level exemptions—specifically for HIPAA and GLBA—to narrower data-level ones.[13] The report stated that the law's numerous broad exemptions were presenting enforcement challenges and that one-third of consumer complaints to the AG in the first six months were unactionable because of various exemptions.[14] If a federal comprehensive bill does try to create carveouts for these laws, they should be data level rather than entity level.[15]

IV. Data Security

A. How can such a law improve data security for consumers? What are appropriate requirements to place on regulated entities?

Consumers are facing an epidemic of data breaches and resulting identity theft and harm due to a lack of investment in and commitment to data security. We have seen that companies will not adequately invest in data security unless they face significant consequences for a failure to do so. Any federal privacy law should adopt a duty of care approach to the consumer data that they collect; if they can't protect it, they shouldn't collect it. And a strong data minimization rule should require that companies only retain data as long as reasonably necessary to effectuate the purpose for which the data was collected, with certain limited exceptions.

---

[13] Conn. Office of the Att'y Gen., Report to the General Assembly's General Law Committee Pursuant to Public Act 22-15, "An Act Concerning Personal Data Privacy and Online Monitoring" Referred to as the Connecticut Data Privacy Act ("CTDPA"), (Feb. 1, 2024), https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf.

[14] *Id.*

[15] *See, e.g.*, S.B. 619, 82d Leg. Assembl., 2023 Reg. Sess. (Or. 2023) (data-level exemptions for HIPAA and GLBA); Cal. Civ. Code §§ 1798.100–1798.199.100 (data-level exemptions for HIPAA and GLBA); Md. Code Ann. Com. Law § 14-4603(B) (data-level exemption for HIPAA).

A federal privacy law should also either give rulemaking authority to an expert agency to detail data security requirements or codify the best practice standards which have been articulated to the business community with consistency over the last decade.[16] Minimum standards with flexibility as to implementation will provide the guardrails necessary to protect consumers from weak data security but prevent the law from becoming outdated and allow industry to innovate on data security in response to evolving cyber threats.

Although all organizations should do some measure of ongoing security review, for organizations possessing a large volume of data or particularly sensitive data, an independent auditor should be responsible for assessing compliance, and their assessment should be technical, be public, use audit-like standards, and allow for external stakeholder input. High-risk organizations should not be allowed to "grade their own homework."

V. Artificial Intelligence

A. How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?

A federal comprehensive data privacy law is a critical first step in reducing harms caused by AI. In terms of AI-specific regulation, states are still in the early stages of exploring various legislative approaches, and Congress should allow that work to continue. Any federal action on AI should set a floor for states and should not impose a ceiling.

VI. Accountability & Enforcement

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

Expert agencies are well positioned to craft regulations implementing a federal privacy law, but those agencies do not have sufficient resources to ensure a law is adequately enforced. The scope of data collection online is too vast for government alone to regulate. This is why previous proposals such as the American Data Privacy and Protection Act and American Privacy Rights Act included a three-tier enforcement mechanism.

Individuals who use online services are in the best position to identify privacy issues and take action to protect their privacy. A private right of action preserves government resources, and the threat of statutory damages is a strong motivator to incentivize compliance with the law.

[16] *See, e.g., Stick with Security: A Business Blog Series*, Fed. Trade Comm'n (2015), https://www.ftc.gov/business-guidance/privacy-security/stick-with-security-business-blog-series; *Cybersecurity Basics,* Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/basics.

A private right of action is the most important tool legislatures can give to their constituents to protect their privacy. Many federal privacy laws include a private right of action, and these provisions have historically made it possible to hold companies accountable for their privacy violations. A private right of action ensures controllers have strong financial incentives to comply with privacy laws. We have seen evidence of this in Illinois,[17] 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.[18]

In contrast, in states where Attorneys General have sole enforcement authority, we have seen little enforcement of (and compliance with) privacy laws.[19]

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?

Agencies tasked with enforcement will need the resources to hire specific teams with expertise in privacy, technology, and data security to enforce privacy laws. They will also need resources to conduct monitoring and investigations. Without dedicated funding and staff, privacy laws are likely to go largely unenforced—there has been only a handful of enforcement actions under state privacy laws,[20] despite more than a dozen of the 19 state privacy laws having already gone into effect.[21] Importantly, the two states that have undertaken enforcement actions under

[17] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf.
[18] 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.
[19] *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, *Companies Continue to Share Health Data Despite New Privacy Laws* (Jan. 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf.
[20] *Honda Settles with CPPA over Privacy Violations*, Cal. Privacy Prot. Agency (Mar. 12, 2025), https://cppa.ca.gov/announcements/2025/20250312.html; *Privacy Enforcement Actions*, Cal. Office of Att'y Gen., https://oag.ca.gov/privacy/privacy-enforcement-actions; Press Release, *Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling over 45 Million Americans' Driving Data to Insurance Companies*, Tex. Office of the Att'y Gen. (Jan. 13, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45.
[21] C Kibby, *US State Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

their state privacy law—Texas and California—both have dedicated teams that focus specifically on privacy enforcement.[22]

C. How could a safe harbor be beneficial or harmful in promoting compliance with obligations related to data privacy and security?

Self-regulatory safe harbor systems in privacy laws have not been successful in the past. Experience with the safe harbor in the Children's Online Privacy Protection Act has demonstrated that safe harbors do not lead to meaningful compliance with the law and prevent enforcement. Congress should not bother enacting a privacy law only to outsource oversight of that law to private companies who have little incentive to enforce the rules where it could lead to clients choosing another safe harbor provider.

A more limited form of best practices guidance or the development of common standards could help companies with compliance while still retaining governmental enforcement authority.

VII. Additional Information

EPIC recommends the following resources to the Working Group:

- **EPIC and Consumer Reports: The State Data Privacy Act**
  Model bill using the Connecticut Data Privacy Act as base text
  https://epic.org/the-state-data-privacy-act/

- **EPIC and U.S. PIRG Education Fund: The State of State Privacy**
  Report scoring existing state privacy laws
  https://epic.org/state-of-privacy-2025

- **Caitriona Fitzgerald and Kara Williams, *Data minimization is the key to a meaningful privacy law* (May 2024)**
  https://epic.org/data-minimization-is-the-key-to-a-meaningful-privacy-law/

[22] *About CPPA*, Cal. Privacy Prot. Agency, https://cppa.ca.gov/about_us/; Press Release, *Attorney General Ken Paxton Launches Data Privacy and Security Initiative to Protect Texans' Sensitive Data from Illegal Exploitation by Tech, AI, and Other Companies*, Tex. Office of the Att'y Gen. (June 4, 2024), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-data-privacy-and-security-initiative-protect-texans-sensitive.