



Electronic Frontier Foundation Response to the Energy and Commerce Committee Privacy Working Group Request for Information

Executive Summary:

American consumers need a strong federal privacy law. EFF appreciates the Committee's efforts to protect the privacy and civil rights of all American consumers. New technologies are advancing our freedoms, but they are also enabling unparalleled invasions of privacy that federal laws have yet to catch up to.

Regulators are increasingly concerned about the harms that stem from a lack of comprehensive privacy law in the US, and for good reason – a lack of updated privacy laws implicate child safety, journalism, access to healthcare data, digital justice, competition, artificial intelligence, and government surveillance, just to name a few. No one wants to live in a world where children are preyed upon, we lose access to news, or we face turbocharged discrimination or monopoly power. It's long past time to pass legislative solutions that are concrete, ambitious, and fully protective of all Americans' data privacy.

Trouble is, previous proposals aimed at the technology industry have often seemed to lose the forest for the trees, with scattered and disconnected bills addressing whichever perceived harm is causing the loudest public anxiety in any given moment. Too often, those proposals do not carefully consider the likely unintended consequences nor even whether the law will reduce the harms it's supposed to target. For example, legislators at the state and federal levels are trying to require private companies to ensure that people (or just children) never see things that those lawmakers don't want them to see online. Yet the legislation almost always runs afoul of the Constitution and human rights standards. It leaves the decisions about what constitutes a "harm" to elected officials, who can vary wildly in their views. It's also unworkable in practice and likely to harm the very people we want to protect.

The truth is many of the ills of today's internet have a single thing in common: They are built on a system of corporate surveillance. Multiple companies, large and small, collect data about where we go, what we do, what we read, who we communicate with, and so on. They use this data in multiple ways and, if it suits their business model, may sell it to anyone who wants it — from law enforcement to data brokers that facilitate elder fraud schemes.



Addressing the core issue of corporate surveillance will better promote human rights and civil liberties – while simultaneously holding space for free expression, creativity, and innovation – than many of the issue-specific bills we’ve seen over the past decade. In other words, whatever online harms you want to alleviate, you can do it better and with a broader impact if you do privacy first.

Breaking It Down: What Does Comprehensive Data Privacy Legislation Look Like?

Comprehensive, well-written data privacy rules will preserve the critical right to user privacy, secure the free expression that privacy enables, and protect information security. Specifically, it must include the following components:

- **No online behavioral ads.** Companies must be prohibited from targeting ads to a person based on their online behavior. These ads are especially dangerous, because they incentivize businesses to harvest as much consumer data as possible, either to use it to target ads or to sell it to someone who will, including bad actors.
- **Real minimization.** Companies must be prohibited from processing a person’s data, except as strictly necessary to provide them whatever product or service they asked for.
- **Strong opt-in consent.** Companies must be prohibited from collecting, retaining, using, processing, or sharing a person’s data, except with their informed, voluntary, specific, opt-in consent. If a consumer consents to collection of their information (such as location data to map a running route for a fitness tracker) for one purpose, companies must get additional consent before selling or using data for another purpose.
- **User rights.** Users should have the rights to access their data, to port it, to correct it, and to delete it. These basic rights have been added to many data privacy laws and date back to a seminal 1973 government report that outlined basic fair information practices.
- **No preemption by a federal law.** Federal privacy law must be a floor and not a ceiling. States must be free to enact privacy laws that are stronger than the federal baseline, and to meet the challenges of tomorrow that are not foreseeable today.



- **Strong enforcement with meaningful impact.** People must have a private right of action to sue the corporations that violate their statutory privacy rights. Remedies must include liquidated damages, injunctive and declaratory relief, and attorney fees. People must be able to bring their claim to a judge, and not be forced into compelled arbitration.
- **No pay-for-privacy schemes.** Just as you shouldn't have to trade your privacy for the ability to use a service at all, you shouldn't have to pay extra for the ability to use it without being surveilled. Privacy must not be a commodity that only the wealthy can afford. This safeguard is necessary to ensure that "consent" is truly voluntary.
- **No deceptive design.** Companies must be prohibited from presenting people with user interfaces (sometimes called "dark patterns") that have the intent or substantial effect of impairing autonomy and choice. This protection is also necessary to ensure that consent is genuine.

Digging in on the Details:

Federal Consumer Privacy Legislation Should be the Floor, not the Ceiling:

Strong baseline federal privacy legislation would benefit consumers across the country, but any action that supplants stronger state laws would hurt consumers and prevent states from protecting their constituents. California's Consumer Privacy Act, Vermont's Data Broker Act, and Illinois' Biometric Information Privacy Act are just a few of the state laws that already protect consumers, and other states are looking at similar proposals. These laws are working.

Congress should reject calls to strip Americans across the country of these state protections in the name of creating a single federal standard. While Americans need federal legislation that protects consumer data privacy, such legislation cannot come at the price of preemption of stronger state laws. Unfortunately, previous iterations of comprehensive privacy bills, such as the American Privacy Rights Act and the American Data Privacy and Protection Act, would preempt many state privacy laws. The Committee should include language in any future bill to clarify that the bill does not preempt any state laws, with the sole exception of state laws that conflict with the federal bill, and then only to the extent of the conflict.



At the very least, the Committee must dramatically expand the list of non-exempted categories of state laws. Any bill should not preempt many existing kinds of state data privacy laws, including:

- state constitutional guarantees of data privacy;
- state limits on when private entities may disclose their customers' data to the government;
- state protections of biometric and genetic privacy;
- state mandates on online businesses to comply with device settings, like browser signals, that opt-out of data processing; and
- state laws that establish privacy protection agencies.

No Weakening Current Federal Privacy Laws

Existing federal statutes and regulations place privacy and other important limits on phone companies and other common carriers. These include the Communications Act of 1934. Creating new protections for the public should not require the dismantling of existing protections.

Previous drafts of privacy bills have taken a significant step backwards for regulation of common carriers, including preempting many parts of the federal Communications Act such as provisions that limit a telephone company's use, disclosure, and access to customer proprietary network information, including location information. This could have ramifications extending far beyond data privacy.

Strong Enforcement

Any strong federal data privacy legislation must contain the most important enforcement tool: the right for consumers to enforce their privacy rights in court. It is not enough for the government to pass laws that protect consumers from corporations that harvest and monetize their personal data. It is also necessary to ensure companies do not ignore them. The best way to do so is to empower ordinary consumers to bring their own lawsuits against the companies that violate their privacy rights. Strong "private rights of action" are among EFF's highest priorities in any data privacy legislation.

Government agencies often lack the resources to enforce existing laws. A private right of action would ensure government agencies or consumers themselves can enforce any protections Congress designs. Many privacy statutes contain a private right of action,



including federal laws on wiretaps, stored electronic communications, video rentals, driver's licenses, credit reporting, and cable subscriptions. So do many other kinds of laws that protect the public, including federal laws on clean water, employment discrimination, and access to public records.

Consumers must also have a real chance to use a private right of action. People often effectively give up such rights when they supposedly “agree” to waive them in terms of service and end user license agreements that they haven't read—and aren't expected to read. Strong data privacy law should prohibit waivers and mandatory arbitration requirements, which allow companies to sidestep the users' rights.

Reject “Pay For Privacy” Schemes

Privacy is a fundamental human right. A federal privacy law must recognize this by including a non-retaliation rule that says companies cannot deny goods, charge different prices, or provide a different level of quality to those who exercise their privacy rights. Without this rule, pay-for-privacy systems will make privacy a luxury and exclude lower income consumers from any intended protections. The American Data Privacy and Protection Act began well on this issue. Strong language must prohibit a covered entity from responding to a person's exercise of their rights by providing them with a different quality of service (in addition to the current prohibitions on denying or terminating their service or charging them a different price).

Prohibit Online Behavioral Advertising

Strong, comprehensive privacy legislation must prohibit companies from targeting ads to consumers based on their online behavior. This dangerously pervasive practice fuels a billion-dollar industry that is largely unregulated. Online behavioral advertisers rely on technical systems that capture enormous quantities of Americans' sensitive information. This information is then widely and recklessly shared to the highest bidder. For example, a recent enforcement action¹ by the Federal Trade Commission shows the dangers of real-time bidding auctions used to place online ads. The sanctioned data broker company collected data on over a billion people, with most coming from advertising auctions. The company then sold this sensitive data for a range of invasive purposes, including tracking people at political protests, and compiling home addresses of healthcare employees for recruitment by competing employers. It also categorized people into custom groups for advertisers, such as “pregnant women,” and “Hispanic churchgoers.”

¹ <https://www.eff.org/deeplinks/2025/01/online-behavioral-ads-fuel-surveillance-industry-heres-how>



This data also can and has been sold to foreign adversaries.² Google’s ad auctions sent sensitive data to a Russian ad company³ for months after it was sanctioned by the U.S. Treasury. These privacy violations are not just occasional missteps—they’re inherent to the business model of online behavioral advertising.

Alternatively, advertisements can be targeted contextually—based on the content of the page you’re currently viewing—without collecting or exposing sensitive information in the way that behavioral advertising does.

Privacy Safeguards

Big businesses are harvesting and monetizing our personal data on an unprecedented scale. Because our nation’s privacy laws have not kept up, these companies are free to put their profits before our privacy. They build increasingly comprehensive dossiers about our lives, choices, and preferences using shadowy and sophisticated technologies to scrutinize our movements, online “clicks,” and personal relationships. This is a grave menace to our privacy and other liberties. Strong and comprehensive data privacy laws promote security, privacy, and free expression. These laws move us forward in the fight to protect children, support journalism, advance access to health care, foster digital justice, limit government surveillance, and strengthen competition.

In sum, legislation must require companies to:

- Minimize their processing of consumers’ data, i.e., process it only as strictly needed to give consumers what they asked for;
- Obtain real consent, and tell consumers what personal information they have collected about them;
- Provide consumers a machine-readable copy of their data and provide consumers a right to correct and delete their data; and
- Congress should also enact a tailored ban on targeted ads based on our online behavior. Removing this incentive to collect and sell as much of our behavioral information as possible would reduce the temptation for bad actors to violate the privacy of American consumers.

² <https://epic.org/wp-content/uploads/2025/01/EPIC-ICCL-Enforce-In-re-Googles-RTB-Complaint.pdf>

³ <https://www.propublica.org/article/google-russia-rutarget-sberbank-sanctions-ukraine>



Thank you again for your leadership on this important topic that impacts the privacy and civil rights of all American consumers. We look forward to working with you to develop comprehensive, well-written data privacy rules that will preserve the critical right to user privacy, secure the free expression that privacy enables, and protect information security.

If you have any questions, please contact Assistant Director of Federal Affairs Maddie Daly at Maddie@eff.org.