epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony of

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)

Hearing on "Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law"

Before the
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy & Commerce

United States House of Representatives

June 3, 2026

Chair Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee, thank you for the opportunity to testify today on the SECURE Data Act. My name is Caitriona Fitzgerald, Deputy Director at the Electronic Privacy Information Center, or EPIC. EPIC is an independent nonprofit established in 1994 to secure the fundamental right to privacy in the digital age for all people. We believe privacy is a fundamental human right.

There is broad bipartisan agreement that Americans need stronger privacy protection. Polls consistently show that consumers across the political spectrum are tired of the status quo.[1] Americans do not want grocery stores using personalized pricing to determine just how much they will tolerate paying for a carton of eggs.[2] Consumers using an app to compare gas prices do not want their location sold to increase their insurance rates.[3] And none of us want U.S. forces in war zones surveilled and targeted by adversaries using data collected for targeted advertising.[4]

We can have a thriving digital economy in the United States while protecting privacy. We know what is needed: strong data minimization, heightened protections for sensitive data, limits on data discrimination, and robust enforcement. That is the direction this Committee should take.

My testimony today covers three main points: First, the SECURE Data Act's approach is fundamentally flawed and does not address the privacy issues Americans face today, but the solutions to do so exist. Second, legislation that combines weak rules with broad preemption of state laws is worse than no federal data privacy law at all. And third, the fact that similar laws have been passed in some red and blue states should not be seen as an endorsement of their consumer protections, but rather a statement on Big Tech's influence.

America needs a strong federal data privacy law. But the SECURE Data Act is not the right approach. This Committee previously advanced bipartisan bills to limit data collection and protect Americans from abusive data tracking. In those negotiations, both sides worked to craft a federal bill that was stronger than the strongest state law. The SECURE Data Act, which came out of a one-sided process, does the opposite. It sets a weaker standard than the weakest state law as the national ceiling. It imposes sweeping preemption to strip privacy rights from millions of Americans in states with stronger protections. In our federalist system, Congress' role should not be to eviscerate hard-fought rights that states have secured for their citizens.

---

[1] Pew Research Center, *How Americans View Data Privacy* (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[2] United Food and Commercial Workers (UFCW) Int'l Union, *Voters Say No To Digital Price Tags & Surveillance Pricing* (May 26, 2026), https://www.ufcw.org/wp-content/blogs.dir/61/files/2026/05/GBAO-UFCW-National-Survey-Memo-052626.pdf.
[3] Jonathan Stempel, Texas sues Allstate for collecting driver data without consent (Jan. 13, 2025), https://www.reuters.com/technology/texas-sues-allstate-over-data-collection-cellphones-2025-01-13/.
[4] Letter from Sen. Ron Wyden to Kirsten A. Davies, CIO, Dept. of Defense (May 28, 2026), https://www.wyden.senate.gov/imo/media/doc/wyden_led_letter_to_dod_cio_kirsten_adavies.pdf.

1. The SECURE Data Act is fundamentally flawed and does not address the privacy issues Americans face today.

A. The SECURE Data Act does not require real data minimization.

The SECURE Data Act includes baseline consumer rights that should be part of any privacy law – the right to access, correct, and delete your data and the right to opt out of certain harmful data practices. But a good privacy law must do more. Those rights put the onus on individual consumers to protect their own privacy rather than implementing clear rules that protect our collective right to privacy. A good privacy law must put obligations on the companies that collect, use, and profit from our personal data. The SECURE Data Act fails to do that.

Supporters of this bill point to its "data minimization" section as providing an important new protection. But the language of that section is not new and would not actually protect privacy at all. A data minimization rule only works if it limits how much data companies can collect and how they can use it, which the SECURE Data Act fails to do.

Instead, the SECURE Data Act says controllers need only limit the collection of personal data to purposes *disclosed to the consumer*. This reinforces the failed status quo of "notice and choice" – businesses can collect and use data for any reason as long as they disclose it in a privacy policy that few consumers read or understand. In fact, it incentivizes companies to list as many purposes as possible, as broadly as possible in their policies, to cover every reason they might ever use data. And the only "choice" a consumer has is to avoid the service.

This so-called choice is illusory in daily life. My 8-year-old loves soccer, and every league he joins requires me to download a new app to see the schedule. If I do not agree with the app's terms, there is no "disagree" button. I must accept the terms, no matter how exploitative, or not use the app. Am I supposed to tell my son he can't play soccer because his mom doesn't want her personal data used to train AI systems? We should not bake this unfair system into law.

The Connecticut Attorney General has called the similar rule in the Connecticut Data Privacy Act an "exploitable standard." In his 2024 Enforcement Report, he said:

> Unfortunately, the CTDPA's current notice-and-consent model sets an exploitable standard— businesses can seek to justify unnecessary data collection by deeming such collection "adequate, relevant and reasonably necessary" to the purposes disclosed to consumers. This standard contravenes data minimization principles outright— it allows businesses to collect data they simply do not need so long as it is disclosed in privacy notices that are often bulky, confusing, or worse, misleading.[5]

[5] Att'y Gen. of the State of Conn, *Updated Enf't Rep.t Pursuant to Conn. Data Privacy Act, Conn. Gen. Stat. § 42-515, et seq.* (Apr. 2025), https://portal.ct.gov/-/media/ag/reports/ctdpaenforcementreportcy2024.pdf.

The Attorney General recommended amending the law to mirror the Maryland Online Data Privacy Act, which limits collection to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer, with a heightened "strictly necessary" standard for sensitive data. Maryland's data minimization standard was based on language from the American Data Privacy and Protection Act ("ADPPA") that passed this Committee on a vote of 53 to 2. Any federal privacy law should take a similar approach.

We know how to address the problems Americans face online today, and language in previous bipartisan bills went a long way toward doing so. The rules in the SECURE Data Act are too permissive and give a green light to Big Tech's harmful business practices.

B. The SECURE Data Act does not adequately protect sensitive data.

Americans' sensitive personal information should not be sold to the highest bidder. A federal privacy law should limit the collection and use of sensitive data to what is strictly necessary for the product or service requested by the consumer and ban the sale of sensitive data. This would allow companies to use sensitive data for legitimate business purposes while eliminating harmful practices that serve only to increase profits rather than benefiting consumers.

Yet the SECURE Data Act allows companies to collect, use, and sell Americans' sensitive data as long as they obtain consent. Opt-in consent alone, especially as weakly defined in this bill, does not adequately protect Americans online.

Checking a box to accept lengthy terms of service is not meaningful consent. Yet under the SECURE Data Act, companies do not have to separate consent requests. Necessary purposes, such as collecting payment information, are listed in the same document as unnecessary purposes, such as data sales. As a result, consumers are often forced to choose between surrendering their personal data and losing access to essential services. Many states specify that consent does not include acceptance of a general or broad terms of use or similar document, but the SECURE Data Act does not include that protection.

The bill also omits prohibitions on "dark patterns" – manipulative designs meant to subvert choice – that exist in over a dozen state laws. This means that a website can offer one easy-to-see, brightly colored "accept" button while hiding "disagree" in a small, hard-to-read font that requires toggling a dozen buttons. When design choices discourage consumers from exercising privacy rights, they undermine the purpose of a privacy law: empowering consumers.[6] The SECURE Data Act makes this version of "consent" the only protection consumers have against the use of their sensitive data, but in practice it is no protection at all.

[6] EPIC, *Good Luck Opting Out: Manipulative Design Patterns in Opt-Out Processes* (May 2026), https://epic.org/good-luck-opting-out-manipulative-design-patterns-in-opt-out-processes-2/.

The move towards more protective standards for sensitive data that do not rely solely on consent is a clear trend among states. Maryland, Oregon, Virginia, and Connecticut have banned the sale of some – or, in Maryland's case, all – categories of sensitive information. Maryland also requires the collection and use of sensitive data to be strictly necessary for the product or service the consumer is requesting. The SECURE Data Act strips residents of those states of their existing protections and gives companies a permission slip to sell our most sensitive personal information for profit.

C. The SECURE Data Act will make minors less safe online.

Many existing state privacy laws provide strong protections for minors online. Numerous states limit targeted advertising to minors and the sale of their personal data.[7] All 22 state privacy laws allow children and teens the right to access, delete, or correct their own personal data, just as adult consumers. The SECURE Data Act does neither.

The SECURE Data Act also contains rules for teens that are practically unworkable. The bill requires companies to obtain verified parental consent before processing any teens' personal data. This requirement would mean that every time a company wants to collect or use a teen's personal data, they would need to obtain parental consent before doing so. This standard would make it nearly impossible for teens to use the internet and would inundate parents with constant pop-ups they will quickly tire of, and therefore likely ignore. This would degrade essential internet services for teens and their parents without any meaningful privacy benefit.

The SECURE Data Act also makes millions of minors less safe online by preempting dozens of existing state laws aimed at protecting minors online. I have attached a list of these laws to my testimony.

The bill's sweeping preemption provisions could also prevent many pending lawsuits seeking to hold companies accountable for privacy violations from moving ahead. Last week, Meta, Snap, YouTube, and TikTok agreed to a $27 million settlement in a lawsuit with a Kentucky school district. The district claimed that the platforms' addictive designs harmed students' mental health.[8] Many of the claims in that case relied on personalized feeds and features, citing the companies' privacy policies. Because the claims "relate to" rules in the SECURE Data Act, defendants in similar cases would likely argue that such claims are preempted. The bill's preemption provisions would risk blocking parents, school districts, and others from holding Big Tech accountable for harms to minors.

---

[7] *See e.g.,* Ark. Code Ann. § 4-88-16; Del. Code Ann. tit. 6 § 12D; 2026 S.C. Acts No. 96.
[8] Diana Novak Jones, *Social Media Companies to Pay $27 Million to Settle Kentucky School District's Lawsuit, Records Show,* Reuters (May 29, 2026), https://www.reuters.com/business/meta-paid-9-million-settle-kentucky-school-districts-lawsuit-over-social-media-2026-05-29/.

Federal privacy law should limit the collection and processing of minors' personal data to what is strictly necessary to provide the product or service they are asking for. It should also ban targeted advertising to minors and prohibit the sale of minors' data.

D. The SECURE Data Act is missing many key protections that exist in state privacy laws.

In addition to lacking real data minimization or adequate protections for sensitive data and minors, the SECURE Data Act is also missing many other key protections that exist in state privacy laws. The bill's broad preemption rules means that Congress would be trampling on state rights, stripping millions of Americans of rights they already have. Such protections include:

- Twelve states require companies to honor universal opt-out mechanisms (UOOMs), which allow consumers to use a one-click setting in their browser to signal to websites that they want to opt out of targeted advertising and the sale of their personal data. Browsers and websites have already implemented the technology to recognize UOOMs because 80 million Americans are protected by state laws that require companies to do so. The SECURE Data Act does not require companies to honor UOOMs and instead gives the Secretary of Commerce three years to issue a report about whether this tool – that already exists and is in widespread use – is feasible.
- Residents of Delaware, Maryland, Minnesota, and Oregon have the right to request businesses tell them either the specific identities of the third parties to whom they disclose a consumer's personal data or, at minimum, give consumers a list of the categories of third parties to whom they disclose personal data. The SECURE Data Act does not include this right.
- The bill does not require companies to conduct data protection assessments to ensure their data processing activities are more beneficial than harmful for consumers. Nineteen of the 22 state privacy laws require companies to conduct such assessments.
- The bill contains weaker definitions of sensitive data, sale of personal data, profiling, publicly available information, de-identified data, and consent then many state privacy laws.

The federal government typically does not pass laws that take away rights from Americans that their state legislators have determined they should have. But that is exactly what this bill does.

E. The SECURE Data Act's lack of a private right of action is particularly problematic given the bill's focus on individual consumer rights.

Robust enforcement is the backbone of meaningful privacy protection. Without a real threat of enforcement, entities can simply ignore the law. A strong privacy law should include both a private right of action and enforcement authority for federal and state authorities. The

SECURE Data Act does not include a private right of action, and it ties the hands of state and federal enforcers with a mandatory right to cure.

The SECURE Data Act's lack of a private right of action is at odds with its focus on individual consumer rights. Americans will have no recourse if a company fails to respond to their access, correction, deletion, or opt-out requests, as government enforcement typically addresses systemic issues rather than individual claims.

A private right of action is a common remedy in consumer protection laws. The Cable Communications Policy Act, Video Privacy Protection Act, Fair Credit Reporting Act, and Driver's Privacy Protection Act all include private rights of action with statutory damages. Previous bipartisan bills, such as ADPPA and the American Privacy Rights Act ("APRA"), contained a heavily negotiated compromise private right of action that allowed individuals to seek injunctive relief and actual damages. The SECURE Data Act threw that compromise out, leaving individuals without a means of enforcing their own privacy rights and isolating itself from other consumer protection laws.

The SECURE Data Act would also hamstring the Federal Trade Commission and state Attorneys General by prohibiting them from initiating any action for a violation of the law until they have provided written notice to the violator and afforded them a right to cure for 45 days. This means that no matter how egregious the violation – for example, Texas' suit against Allstate Insurance for secretly collecting and selling location data – federal and state enforcers could not penalize the offending company as long as they "fix" the problem within that 45-day window, even though the damage is already done. Many states have either given enforcers the discretion to offer a right to cure or have sunset mandatory rights to cure one to two years after the law goes into effect. The SECURE Data Act does not take either of these approaches; instead, it again includes the most permissive option.

2. Legislation that combines weak rules with broad preemption of state laws is worse than having no federal data privacy law at all.

A strong privacy law should work with, not against, established state protections. The SECURE Data Act would freeze outdated standards into law while hitting the delete button on decades of state laws related to privacy, data security, civil rights, and kids' online safety. Rather than advancing consumer rights, its passage would cement weak rules into law, deter stronger future laws,[9] and leave Americans more vulnerable than ever. **Passage of the SECURE Data Act would put many Americans in a worse position than they are in now, making the enactment of this bill worse than no federal privacy law at all.**

[9] *See* Montesquieu, *The Spirit of the Laws* (1748) ("Useless laws weaken the necessary laws.").

EPIC supported the bipartisan proposals in ADPPA and APRA even though those bills included preemption provisions we did not agree with. We did so because we felt the substantive rules in those bills were largely stronger than existing state laws and would protect Americans from data abuse even as technology evolved. That is not the case with the SECURE Data Act, which is weaker than existing state privacy laws, yet includes broader preemption. This is fundamentally backwards in a federalist system.

In privacy and consumer protection law, federal ceiling preemption is an aberration. Federal consumer protection and privacy laws, in general, serve as regulatory baselines and do not prevent states from enacting and enforcing stronger protections. The sectoral laws that have filled the gap left by the lack of a federal comprehensive data privacy law all allow states to craft protections that exceed federal law. This includes the:

- Electronic Communications Privacy Act;
- Right to Financial Privacy Act;
- Cable Communications Privacy Act;
- Video Privacy Protection Act;
- Employee Polygraph Protection Act;
- Driver's Privacy Protection Act;
- Gramm-Leach-Bliley Act; and
- Fair Credit Reporting Act.

Despite floor preemption in these laws, there has not been a wave of state laws related to these issues.

In contrast, the SECURE Data Act contains an extraordinarily broad preemption standard known as "relating to" preemption. A recent Congressional Research Service (CRS) report on "Preemption & Privacy Law" noted that "the Supreme Court has characterized these 'related to' provisions as 'deliberately expansive' and 'conspicuous for [their] breadth.'"[10] The CRS report goes on to describe other terms Congress could use to limit the scope of a preemption clause, but the SECURE Data Act contains the most expansive option.

Conflict preemption has been sufficient in other privacy regimes, and there is no reason it cannot work in comprehensive federal privacy legislation. Most states already operate under 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 deter states from enacting laws until changes in technology necessitate it.

I have attached a representative list of privacy, security, online safety, civil rights, and AI accountability state laws that EPIC believes could be preempted by the SECURE Data Act's broad preemption provision.

[10] Chris D. Linebaugh, Cong. Rsch. Serv., R48667, Preemption and Privacy Law (2025), https://www.congress.gov/crs_external_products/R/PDF/R48667/R48667.2.pdf.

3. The fact that similar laws have been passed in some red and blue states should not be seen as an endorsement of their consumer protections, but rather a statement on Big Tech's lobbying power.

The SECURE Data Act has been said to follow the "successful model many red, blue, and purple states have already enacted into law."[11] But these laws have ***not*** been successful for consumers. Rather, they have been successful in giving the businesses profiting off Americans' personal data a permission slip to continue doing so. **Civil society groups, including leading consumer and privacy organizations, have long opposed these bills.**[12]

Many of these state laws closely follow a model initially drafted by tech giants.[13] This model first emerged in Washington in 2019, but did not pass.[14] An Big Tech lobbyist encouraged a Virginia lawmaker to introduce a similar bill, which became law in 2021.[15] In a scorecard released by EPIC and U.S. PIRG Education Fund, Virginia's law received an F.[16] Unfortunately, that permissive Virginia law became the model that lobbying groups funded by Big Tech companies have pushed other states to adopt, and this tactic has succeeded in over twenty states.

Republican Kentucky State Senator Whitney Westerfield had originally introduced a stronger privacy bill, but in a hearing discussing Big Tech's lobbying tactics in 2024, he said:

> The Kentucky Chamber of Commerce, informed by a lot of the biggest players in the country and in the world who are parts of the State Privacy and Security Coalition, the AT&Ts and others, Amazon, and the likes. You had a lot of people demanding that my bill not advance, or something like my bill not advance.[17]

---

[11] H. Comm. on Energy & Commerce, *Chairmen Guthrie and Bilirakis Announce Hearing on Establishing a Federal Data Privacy Law* (May 27, 2026), https://energycommerce.house.gov/posts/chairmen-guthrie-and-bilirakis-announce-hearing-on-establishing-a-federal-data-privacy-law.

[12] *See e.g.,* Consumer Reports, *Consumer Reports Opposes Kentucky H.B. 15, Consumer Privacy Legislation* (Feb. 2024), https://advocacy.consumerreports.org/research/consumer-reports-opposes-kentucky-h-b-15-consumer-privacy-legislation/; EPIC, *EPIC, Coalition Opposes Weak West Virginia Privacy Bill* (Mar. 2025), https://epic.org/epic-coalition-opposes-weak-west-virginia-privacy-bill/; Center for Democracy & Tech., *States are Letting Us Down on Privacy* (Jan. 2024), https://cdt.org/insights/states-are-letting-us-down-on-privacy/.

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

[14] 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/.

[15] Dastin et al., *supra* note 13.

[16] EPIC, *The State of Privacy* (2025), http://epic.org/state-of-privacy-2025.

[17] Hearing before the Vt. H. Comm. on Commerce and Economic Dev. (Apr. 26, 2024), *available at* https://www.youtube.com/live/RfvAteuwRCA?t=3777s (testimony of Ky. State Sen. Whitney Westerfield).

The playbook he described happened in state after state: Big Tech poured money into coalitions, trade groups, and astroturf groups, as well as local business organizations, to push a weak law that enshrines their harmful business practices into law. The SECURE Data Act is even weaker than nearly every one of them.

Some states, such as Maryland, have recently built on these laws and added important consumer protections, such as strong data minimization and a ban on the sale of sensitive data. This Committee should do the same rather than advance a federal bill that is weaker than already-weak state privacy laws.

* * *

Privacy is a fundamental right, and our laws should reflect that. The trends in the U.S. are clear: commercial surveillance systems are collecting and selling increasing amount of our personal data, artificial intelligence is making that exploitation worse, and Americans want more protections from Big Tech. Yet, this Committee is moving in the direction of weaker legislation than it overwhelmingly approved in previous sessions. Congress should not be passing a federal data privacy law that fails to stop the very real data abuses and privacy harms that are happening every minute of every day. And it certainly should not be stripping Americans of privacy rights they already have.

We know what the solutions to these problems look like – federal privacy legislation must include strong data minimization rules, heightened protections for sensitive data, limits on data discrimination, and effective enforcement. The SECURE Data Act unfortunately does not meet the moment, but the solutions exist, and I urge the Subcommittee to consider other approaches that give Americans the privacy they want and deserve.

Thank you for the opportunity to testify today.

Appendix

State laws that would be preempted by the SECURE Data Act

The following is a representative list of state laws that EPIC believes would be preempted by the SECURE Data Act's broad preemption provision, which preempts any state law "that relates to the provisions of this Act." It is not a comprehensive list – there are likely dozens more state laws that would be preempted by the SECURE Data Act.

- Comprehensive privacy laws in **22 states**:
  - Alabama, California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Louisiana, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia
- Invasion of privacy laws (statutory and torts, **all 50 states**) including:
  - Intrusion Upon Seclusion – common law rights where exercised with regard to personal information online (states adopting 2d Restatement of Torts include Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Mississippi, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Tennessee, Texas, Utah, Vermont, Washington, and West Virginia)[18]
  - Eavesdropping and electronic surveillance statutes in nearly all states (Vermont does not have an eavesdropping statute, and the Connecticut statute does not cover electronic communications)
- Laws aimed at protecting minors online:
  - Age-Appropriate Design Codes in **5 states**:
    - California, Maryland, Nebraska, South Carolina, Vermont
  - Arkansas Children and Teens' Online Privacy Protection Act
  - California Protecting our Kids from Social Media Act
  - Connecticut SB 3 and SB 4 (amending the CT Data Privacy Act)
  - Colorado Privacy Protections for Children's Online Data (amending the CO Data Privacy Act)
  - Georgia Protecting Georgia's Children on Social Media Act of 2024
  - Louisiana Secure Online Child Interaction and Age Limitation Act
  - Louisiana Protection of Children's Internet Data
  - Mississippi Walker Montgomery Protecting Children Online Act
  - New York SAFE for Kids Act

[18] Eli A. Meltz, *No Harm, No Foul? "Attempted" Invasion of Privacy and the Tort of Intrusion Upon Seclusion of Intrusion Upon Seclusion*, 83 Fordham L. Rev. 3431 (2015), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5122&context=flr.

    - New York Child Data Protection Act
    - Texas Securing Children Online through Parental Empowerment (SCOPE) Act
    - Utah Minor Protection in Social Media Act
- Laws requiring age assurance to access social media:
    - Arkansas Social Media Safety Act
    - Florida Online Protections for Minors
    - Georgia Protecting Georgia's Children on Social Media Act
    - Nebraska LB383 Parental Rights in Social Media Act
    - Tennessee Protecting Children from Social Media Act
    - Texas SCOPE Act
    - Virginia's social media age verification law
    - Utah Social Media Regulation Act
- Laws requiring device-based filters for harmful content
    - Alabama Act 2025-406
    - Utah Children's Device Protection Act (Laws 2024, Ch. 166)
- Laws requiring age assurance to access "harmful" material that can be proscribed for kids (e.g., pornography) in **25 states:**
    - Alabama, Arizona, Arkansas, Florida, Idaho, Indiana, Kansas, Kentucky, Louisiana, Mississippi, Missouri, Montana, Nebraska, North Carolina, North Dakota, Ohio, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, West Virginia, Wyoming
- App store accountability laws in **4 states:**
    - Texas, Utah, Louisiana, and Alabama
- Device/operating system age assurance
    - California Digital Age Assurance Act
- Health data and genetic privacy laws
    - Washington My Health My Data Act
    - Nevada's Health Data Privacy Act
    - Genetic privacy laws in **11 states:**
        - Texas, Florida, Montana, Tennessee, Virginia, Arizona, Kentucky, Maryland, Utah, Wyoming, Alaska
- Biometric privacy laws
    - Texas Capture or Use of Biometric Identifier Act
    - Illinois Biometric Information Privacy Act
- Robocalls
    - Arizona Do-Not-Call
    - Connecticut Telemarketing Law

    - Florida Telephone Solicitation Act
    - Georgia Telemarketing law
    - Maryland Stop the Spam Calls Act of 2023
    - Mississippi Telephone Solicitation law
    - New Jersey Telemarketing law
    - New York Telemarketing law
    - Oklahoma Telephone Solicitation Act
    - Texas Telemarketing law
    - Tennessee Telephone Solicitation law
    - Virginia Telephone Privacy Protection Act
    - Washington Robocall Scam Protection Act
- ISP privacy
    - Maine Internet Service Provider privacy law
- Data broker laws
    - Data broker registry laws in **4 states** (California, Texas, Vermont, Oregon)
    - California DELETE Act
    - California Opt Me Out Act
- Data security laws
    - At least **25 states** have statutes requiring reasonable data security procedures and practices.[19]
    - Massachusetts data security law (Chapter 93H)
    - Nevada Security and Privacy of Personal Information law
- Data breach notification laws **in all 50 states**
- Laws governing automated decision-making systems
    - Colorado AI Act
    - California's ADMT regulations
- Civil rights laws as applied in cases where personal information is used to facilitate unlawful discrimination
- Laws prohibiting non-consensual distribution of intimate images **in all 50 states**
- Cybercrime / hacking laws
    - Virginia Computer Invasion of Privacy §18.2-152.5
- Unfair and deceptive trade practices – enforcement actions related to privacy and data abuses

[19] Nat'l Conf. of State Legislators, *Data Security Laws,* https://www.ncsl.org/technology-and-communication/data-security-laws-private-sector.

The SECURE Data Act also eliminates existing federal privacy protections

The SECURE Data Act eliminates some of the few federal privacy protections that Americans currently enjoy, including the:

- Video Privacy Protection Act
- Communications Act Section 202(a)
- FCC Digital Discrimination section of Infrastructure Investment and Jobs Act