

The State of Privacy

**How state “privacy” laws fail to
protect privacy and what they can
do better**

**Illinois PIRG Education Fund
Electronic Privacy Information Center (EPIC)
February 2024**

The State of Privacy:

**How state “privacy” laws fail to protect
privacy and what they can do better**

Written by:

Abe Scarr

R.J. Cross

Illinois PIRG Education Fund

Caitriona Fitzgerald

Kara Williams

Electronic Privacy Information Center (EPIC)

February 2024

Illinois PIRG
Education Fund

epic.org /
ELECTRONIC
PRIVACY
INFORMATION
CENTER

Acknowledgements

EPIC wishes to thank Reset Tech Action, who provided funding that supported the work on this report. We also wish to thank our generous donors, who make it possible for us to stand up to Big Tech as an independently funded organization.

Illinois PIRG Education Fund wishes to thank Edmund Coby and Ellen Hengesbach for their substantial research and editorial contributions to this report. We also wish to thank the Rose Foundation for Communities and the Environment for their generous support of our education work and our citizen donors for enabling us to stand up for their rights and the public interest in the long-term.

EPIC and Illinois PIRG Education Fund would both like to acknowledge state legislators and their staffs nationwide: You work tirelessly and diligently, often on tight deadlines and with tight resources, in service of your constituents. You have our respect and our thanks.

The authors bear responsibility for any factual errors. Policy recommendations are those of Illinois PIRG Education Fund and EPIC. The views expressed in this report are those of the authors and do not necessarily reflect the views of our funders or those who provided review.

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) non-profit public interest research and advocacy center in Washington, D.C. EPIC was established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. Our mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. For more information about EPIC, please visit www.epic.org.

With public debate around important issues, often dominated by special interests pursuing their own narrow agendas, Illinois PIRG Education Fund, a 501(c)3 organization, offers an independent voice that works on behalf of the public interest. We investigate problems, craft solutions, educate the public, and offer meaningful opportunities for civic participation, all to better protect the public interest. For more information about Illinois PIRG Education Fund, please visit www.pirg.org/edfund.

Table of contents

- Executive summary..... 3**
- Introduction..... 5**
- The problem: Without rules, data abuse runs rampant..... 7**
 - Many companies collect and use data in surprising — and risky — ways.....7
 - Unchecked data collection puts consumers’ security at risk, turbocharges targeted scams, and increases the odds of identity theft..... 9
 - Data used to profile consumers often leads to discriminatory outcomes.....10
 - Current data practices can inundate consumers with annoying — and even harmful — targeted ads.....11
- Why this is happening: Big Tech is writing the rules..... 13**
- The solution: What a strong privacy law looks like.....16**
 - Features of strong state-level regulations..... 16
 - Data minimization..... 16
 - Strong enforcement..... 18
 - Rulemaking authority..... 19
 - Civil rights protections..... 19
 - Transparency and assessing high-risk data practices..... 19
 - Meaningful individual rights..... 20
 - Banning manipulative design and unfair marketing..... 21
 - Importance of strong definitions..... 22
- Grading on a curve: How state laws fail to protect consumers’ privacy and security..... 24**
 - California: an advancing “B” state..... 25
 - The middling “C” states Colorado..... 26
 - Colorado..... 26
 - New Jersey..... 27
 - Oregon..... 28
 - Delaware..... 29
 - Lagging “D” states..... 30
 - Connecticut..... 30
 - New Hampshire..... 31
 - Montana..... 32
 - The failing “F” states..... 33
 - Texas..... 33
 - Virginia..... 33
 - Indiana..... 33
 - Tennessee..... 33
 - Utah..... 33
 - Iowa..... 33
- Illinois’ opportunity to lead the class.....35**
- Appendix A: Methodology..... 36**
- Appendix B: Grading criteria..... 38**

Weak, industry-friendly laws allow companies to continue collecting data about consumers without meaningful limits. Consumers are granted rights that are difficult to exercise, and they cannot hold companies that violate their rights accountable in court.

Big Tech has played a big role in the passage of weak state privacy bills. Of the 14 laws states have passed so far, all but California's closely follow a model that was initially drafted by industry giants such as Amazon. In an analysis of lobbying records in the 31 states that heard privacy bills in 2021 and 2022, the Markup identified 445 active lobbyists and firms representing Amazon, Meta, Microsoft, Google, Apple, and industry front groups. This number is likely an undercount.

No laws should be written by the companies they are meant to regulate. Allowing Big Tech to heavily shape our privacy rules allows them to consolidate their already outsized power in the economy and in our lives. Privacy rules should balance the scale in favor of the billions of people who rely on the internet in their day-to-day lives.

State	Grade	Score
California	B+	69
Colorado	C+	41
New Jersey	C	37
Oregon	C-	31
Delaware	C-	30
Connecticut	D	24
New Hampshire	D	22
Montana	D	20
Texas	F	16
Indiana	F	11
Virginia	F	11
Utah	F	6
Tennessee	F	6
Iowa	F	4

A strong comprehensive consumer privacy law would:

- impose data minimization obligations on companies that collect and use personal information – taking the burden off of individuals to manage their privacy online and instead requiring entities to limit their data collection to better match consumer expectations;
- strictly regulate all uses of sensitive data, including health data, biometrics, and location data;
- establish strong civil rights safeguards online and rein in harmful profiling of consumers;
- provide strong enforcement and regulatory powers to ensure the rules are followed; and
- enable consumers to hold companies accountable for violations in court.

A better future is possible. As of this writing, states including Illinois, Maine, Massachusetts, and Maryland are considering strong legislation that would force changes to the abusive data practices driving commercial surveillance and online discrimination, while allowing businesses to continue to innovate. We can have a strong technology sector while also protecting personal privacy. And states can lead the way.

Introduction

In today's world, our lives are increasingly lived online. Nearly everything we do is mediated through personal devices, turning every click, search, and purchase we make on our favorite apps and sites into data points that are collected by companies on the other side of our screens.

These companies — many of whom you've never heard of and don't know you're interacting with — have turned your information into a lucrative business model, threatening your data security and privacy along the way.

In the last two decades, an entire invisible economy has materialized made up of thousands of secretive data companies trafficking in the information of nearly every American. Even companies that are household names are increasingly opening new revenue streams by gathering a lot more data from consumers than is necessary and using it for secondary purposes that have nothing to do with delivering the service consumers are expecting to get.¹

Consumers are increasingly aware of the extent of this near-constant data collection, even though in most cases they don't have a way to stop it. Over 80% of Americans are concerned about how companies collect and use their data.² Many are worried that the growth of artificial intelligence will lead companies to use even more personal data in ways people are not expecting and would not be comfortable with.³

Over 80% of Americans are concerned about how companies collect and use their data.

Despite the public's growing unease, meaningful protections for consumers are largely nonexistent. The U.S. still lacks a comprehensive federal privacy law. The few sector-specific laws that do exist — such as the Electronic Communications Privacy Act and the Health Insurance Portability and Accountability Act — were passed in the '80s and '90s, meaning they fail to address 30 years of significant technological changes and increasingly invasive data practices.⁴

For example, HIPAA essentially only covers personal health information in the hands of traditional doctors' offices and insurance companies. Today's healthcare, however, takes place across a

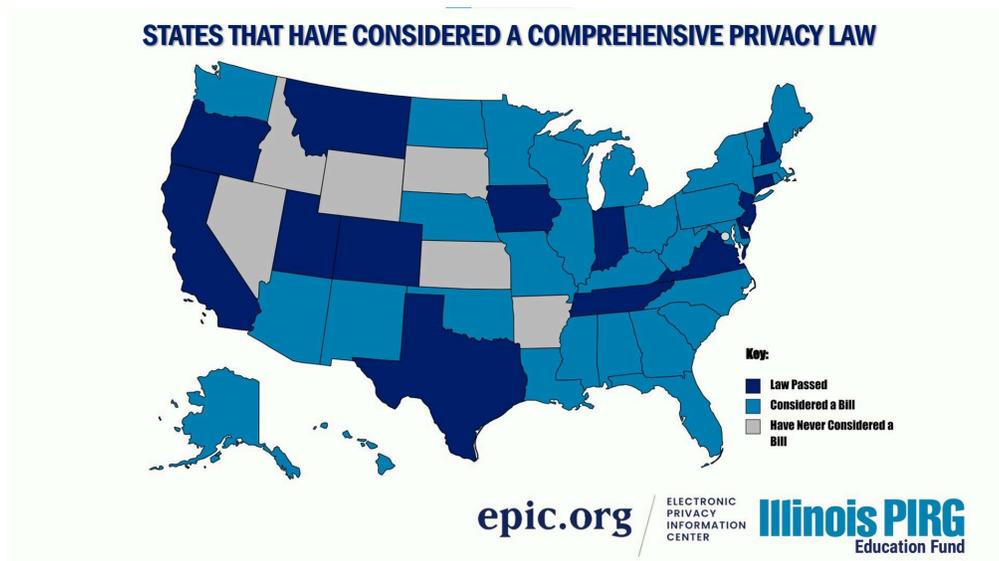
¹ R.J. Cross, *The New Data Brokers: Retailers, Rewards Apps & Streaming Services Are Selling Your Data*, PIRG (June 16, 2023), <https://pirg.org/articles/the-new-data-brokers-retailers-rewards-apps-streaming-services-are-selling-your-data/>.

² Pew Research Center, *How Americans View Data Privacy* (Oct. 18, 2023), <https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/>.

³ *Id.*

⁴ EPIC, *Grading on a Curve: Privacy Legislation in the 116th Congress* (April 2020), <https://epic.org/wp-content/uploads/2022/01/EPIC-GradingOnACurve-Apr2020.pdf>.

fragmented array of websites, smartphone apps, and wearable devices like Fitbits that generate and collect data most Americans would consider sensitive health information on a near-constant basis. Because of HIPAA's narrow scope and its passage before these technologies were in common practice, none of this data is protected, and it can all be mined, bought, and sold for commercial use. This runs understandably counter to the expectations of consumers. A 2023 study found that over 80% of Americans assume that the health data collected by apps is covered by HIPAA, even though it isn't.⁵



This lack of regulation has allowed companies to embed commercial surveillance into every aspect of the web. In the absence of strong federal privacy laws, states have begun to take action. Since 2018, 44 states have considered legislation to protect people's privacy and security. As of February 1, 2024, 14 of those states have passed such laws.⁶

Unfortunately, the vast majority of these statutes fail to give consumers real and meaningful protections and can even end up putting consumers in harm's way. Many of these laws have been heavily influenced by the very industry they seek to regulate. Consumers are told they have "privacy rights," but due to the way the laws are written, those rights are nearly impossible for the average American to exercise. Meanwhile, the laws allow Big Tech to continue amassing and abusing our personal data for its own benefit.

In this report, EPIC and Illinois PIRG Education Fund have come together to shed light on the alarming trend of poor state privacy laws, why these issues affect us all, and what we can do to change course.

⁵ *Many Americans Don't Realize Digital Health Apps Could Be Selling Their Personal Data*, ClearData (July 13, 2023), <https://www.cleardata.com/many-americans-dont-realize-digital-health-apps-could-be-selling-their-personal-data/>.

⁶ Andrew Folks, *US State Privacy Legislation Tracker*, IAPP (Jan. 19, 2024), <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.

The problem: Without rules, data abuse runs rampant

Without meaningful limits on the collection and use of personal data, many companies are incentivized to collect as much data about consumers as possible and to retain it indefinitely. This out of control data collection puts consumers' security and privacy at risk.

Many companies collect and use data in surprising — and risky — ways.

Almost every interaction we have online generates data about us. Sometimes this data collection matches our expectations — Amazon needs your shipping address to send you a package, and Uber needs your location to pick you up. But often, the collection and use of your data is far outside of what you'd expect.

For example, the fast-food chain Tim Hortons was accused by Canadian authorities in 2022 of using its mobile app to harvest users' location data 24/7, even when the app was closed.⁷ And, according to a Mozilla Foundation investigation last year, all 25 major car brands may collect surprisingly intimate data from customers, including in some cases geolocation, health diagnoses, and genetic information using your car's onboard computers and companion apps.⁸

The reality is that tracking systems are embedded in nearly every website you visit and app you download, and they begin to collect information as soon as you connect, tracking your every click, search, and movement across the web.

Companies are incentivized to use our data for purposes that have nothing to do with what we're expecting to get. For example, a 2022 BuzzFeed investigation found the Christian site Pray.com was releasing detailed data about its users with third parties, including Facebook, meaning "users could be targeted with ads on Facebook based on the content they engage with on Pray.com — including content modules with titles like 'Better Marriage,' 'Abundant Finance,' and 'Releasing Anger.'"⁹ A 2022 study by Human Rights Watch found that educational apps and websites used

⁷ Ian Austen, 'A Mass Invasion of Privacy' but No Penalties for Tim Hortons, N.Y. Times (June 11 2022), <https://www.nytimes.com/2022/06/11/world/canada/tim-hortons-privacy-data.html>.

⁸ Jen Caltrider, Misha Rykov & Zoe MacDonald, *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, The Mozilla Foundation (Sept. 6 2023), <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

⁹ Emily Baker-White, *Nothing Sacred: These Apps Reserve The Right To Sell Your Prayers*, BuzzFeed (Jan. 25, 2022), <https://www.buzzfeednews.com/article/emilybakerwhite/apps-selling-your-prayers>.

by schools were harvesting the data of millions of schoolchildren, sending children’s information to data brokers and advertising technology companies while they learned.¹⁰

The reality is that tracking systems are embedded in nearly every website you visit and app you download, and they begin to collect information as soon as you connect, tracking your every click, search, and movement across the web. And with the increasing proliferation of “smart” devices in homes, offices, and other locations, oftentimes your personal data is being collected even when you aren’t intending to interact with an online service at all. Other activities like credit card purchases¹¹ and even physical movements¹² can be logged and tracked without your awareness.

A recent study from the Irish Council for Civil Liberties found that the Real-Time Bidding market, which is where companies exchange user browsing, location, and other data to drive targeted advertising, alone exposes the average American’s data 747 times per day.¹³ This means U.S. internet users’ online activity and location are being tracked and disclosed 107 trillion times per year.¹⁴

These trackers collect millions of data points each day that are sold or transferred to data brokers, who then combine them with other personal data sources to build invasive profiles. Data brokers are shadowy companies that buy, aggregate, disclose, and sell billions of data elements on Americans, all with virtually no oversight.¹⁵ The profiles they build on us are often used to target us with “personalized” advertisements that stalk us across the web. In other cases, these profiles are fed into secret algorithms used to determine the interest rates on mortgages and credit cards, to raise consumers’ interest rates, or to deny people jobs, depriving them of opportunities.

This ubiquitous tracking of everything we do online, and the entities that aggregate and monetize it, poses threats to consumers’ privacy, autonomy, and security. And it shouldn’t be allowed to continue unregulated. The rules we suggest in this report would limit data collection and use to what is *reasonably necessary* for the product or service you’re requesting, better lining up companies’ data practices with your expectations. This would limit cross-site tracking and stop the flow of endless amounts of personal data to data brokers.

¹⁰ Drew Harwell, *Remote Learning Apps Shared Children’s Data at ‘Dizzying Scale’*, Wash. Post (May 24, 2022), <https://www.washingtonpost.com/technology/2022/05/24/remote-school-app-tracking-privacy/>.

¹¹ R.J. Cross, *How Mastercard Sells its ‘Gold Mine’ of Transaction Data* (Sept. 2023), <https://pirg.org/edfund/resources/how-mastercard-sells-data/>.

¹² Michael Kwet, *In Stores, Secret Surveillance Tracks Your Every Move*, N.Y. Times (June 2019), <https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html>

¹³ Irish Council for Civil Liberties, *The Biggest Data Breach ICCL Report on Scale of Real-Time Bidding Data Broadcasts in the U.S. and Europe* (May 2022), <https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf>.

¹⁴ *Id.* at 2.

¹⁵ EPIC, *Data Brokers*, <https://epic.org/issues/consumer-privacy/data-brokers/>.

Unchecked data collection puts consumers' security at risk, turbocharges targeted scams, and increases the odds of identity theft.

The more data companies collect about us, the more our data is at risk. When companies store our information for longer than necessary, or sell it to other entities, it greatly increases the odds that our personal information will be exposed in a breach or a hack. Once exposed, hackers and other bad actors sell information like consumers' names, contact information, bank account information, personal relationship data, and buying habits on underground markets online. Your information can end up on robocall lists or with identity thieves and scammers. The security of our financial accounts can be compromised when hackers have access to the vast tracking data that online companies generate.

In 2022, the FTC received more complaints about identity theft — over 1.1 million complaints from consumers — than any other category.

These problems affect millions of Americans every year. In 2022, the FTC received more complaints about identity theft — over 1.1 million complaints from consumers — than any other category.¹⁶ The second most common complaint was about imposter scams — schemes where fraudsters falsely claim to be a relative in distress,

a business a consumer has shopped at previously, or an authority figure requesting money or personal information. In 2022, consumers lost nearly \$2.7 billion to imposter scams.¹⁷ The more personal information scammers have about a consumer's life, the more convincing these scams become.

Data brokers may even work directly with scammers. Brokers may compile “suckers lists” of ideal victims most likely to fall for certain types of scams. In 2020 and 2021, the U.S. Department of Justice charged three major data brokers for knowingly supplying lists of millions of vulnerable Americans to scammers, including elderly Americans and people with Alzheimer's.¹⁸

The best way to protect consumer data is to not collect, or not store, personal data beyond what is reasonably necessary. Data that is never collected in the first place, or that is quickly deleted, cannot be breached. The most important step states can take to strengthen data security is to enact a comprehensive privacy law that includes a strong data minimization rule.

¹⁶ FTC, *Consumer Sentinel Network Databook 2022* (Feb. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

¹⁷ *Id.*

¹⁸ Alistair Simmons & Justin Sherman, *Data Brokers, Elder Fraud, and Justice Department Investigations*, LawFare (July 25, 2022), <https://www.lawfaremedia.org/article/data-brokers-elder-fraud-and-justice-department-investigations>.

Data used to profile consumers often leads to discriminatory outcomes.

In many cases, the massive collection of data in the hands of data brokers means that consumers are sorted and scored in discriminatory ways.¹⁹ Data brokers build detailed profiles about individuals with information ranging from basic contact information to purchasing habits to sensitive information like race, income, sexuality, and religion. Using raw data, brokers often summarize people with tags such as “working-class mom,” “frequent alcohol drinker,” “financially challenged,” or “depression sufferer.”

Virtually no American is untouched by data brokers. One firm studied by the FTC reported having 3,000 data segments on nearly every U.S. consumer.²⁰ Despite never directly interacting with you, they hold massive amounts of your personal data, which they then use to create your profile.

One firm studied by the FTC reported having 3,000 data segments on nearly every U.S. consumer.

These ever-growing profiles are used to shape customers’ experience of the websites they visit in ways that are entirely opaque to them. These profiles can alter what we see, what prices we pay, and whether we are able to find the information that we seek online (including information about job opportunities, health services, and relationships).

This profiling reinforces discrimination by allowing advertisers to decide who should see a specific product. Advertisers can use characteristics like race, gender, or income (or ZIP code as a proxy for income) to filter their audience and target individuals most likely to buy their product or service. If a company is hiring a CEO, advertisers can choose to show that job opening to only men. If a home is for sale, advertisers can choose to show that listing to only white individuals.

In fact, Facebook was sued by the Department of Housing and Urban Development in 2019 for allowing advertisers to conduct this type of discrimination.²¹ HUD charged Facebook with engaging in housing discrimination by allowing advertisers to control which users saw ads based on characteristics like race, religion, and national origin.²²

¹⁹ See EPIC, Comments to FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security (Nov. 2022), <https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf>.

²⁰ FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-feral-trade-commission-may-2014/140527databrokerreport.pdf>.

²¹ Charge of Discrimination, HUD, et al v. Facebook, Inc., FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

²² *Id.*

Many state laws give consumers the right to opt-out of profiling, which is a step in the right direction. States should also include strong anti-discrimination provisions that prohibit companies from using data in discriminatory ways.

Current data practices can inundate consumers with annoying — and even harmful — targeted advertising.

Massive troves of consumer data flow into the targeted advertising industry. Ads designed to follow users across the Internet can be exhausting and annoying; Americans are inundated with an estimated 5,000 ads daily, up from 500 a day in the 1970s.²³ While consumers can protect their mailboxes from junk mail and phones from spam calls, there's no real recourse for Americans to protect their screens from annoying, distracting, and invasive ads.

Some targeted ads aren't just annoying — they can be predatory and harmful, using people's online behavioral data to reach vulnerable consumers that meet specific parameters. People searching terms like “need money help” on Google have been served ads for predatory loans with staggering interest rates over 1,700%.²⁴ An online casino targeted ads to problem gamblers offering free spins on its site.²⁵ In another example, a precious metals scheme used Facebook users' ages and political affiliations to target ads to get users to spend their retirement savings on grossly overpriced gold and silver coins.²⁶

Advertising can still serve businesses' objectives without relying on the collection and sale of personal data that put consumers unnecessarily in harm's way. Many companies rely instead on contextual advertising, serving ads on podcasts based on the topics discussed and likely audiences they intend to reach based on their interests. For example, a company that sells running shoes would likely find their intended audience by advertising on a health and fitness podcast. This type of rich contextual advertising is the evolution of techniques that were traditionally used in print and broadcast media for decades, and this method doesn't require monitoring of users' browsing history or the creation of individual consumer profiles. And some research shows that consumers prefer contextual ads over specifically targeted ones. A study by Seedtag and Nielsen found that contextual advertising actually increases consumer interest by

²³ USCDornsife, *Thinking vs. Feeling: The Psychology of Advertising* (Nov. 17, 2023), <https://appliedpsychologydegree.usc.edu/blog/thinking-vs-feeling-the-psychology-of-advertising>.

²⁴ Shanti Das, *Google Profiting from 'Predatory' Loan Adverts Promising Instant Cash*, *The Guardian* (Mar. 13, 2022), <https://www.theguardian.com/technology/2022/mar/13/google-profiting-from-predatory-loan-adverts-promising-instant-cash>.

²⁵ Rob Davies, *Online Casino Advert Banned for Targeting Problem Gamblers*, *The Guardian* (Oct. 9, 2019), <https://www.theguardian.com/society/2019/oct/09/casumo-ad-banned-for-targeting-people-trying-to-stop-gambling>.

²⁶ Jeremy B. Merrill, *How Facebook Fueled a Precious-Metal Scheme Targeting Older Conservatives*, *Quartz* (Nov. 19, 2019), <https://www.yahoo.com/video/facebook-fueled-precious-metal-scheme-110044886.html>.

32% and that 85% of consumers who saw contextual ads instead of targeted ads were more open to seeing future ads.²⁷

Much of the pervasive tracking that drives targeted ads is not necessary. Online advertising and other business data uses would look different without it, but businesses would still be able to offer goods and services, and advertising could work fine without it. But Big Tech doesn't want to fix the problem they have created. They built systems that invade our private lives, spy on our families, and gather the most intimate details about us for profit, so they oppose legislation that meaningfully protects your privacy. And because of their outsized influence on state policy, we are left with weak privacy laws that do little to protect consumers. The rules we propose in this report allow companies to continue advertising to their intended customers but in a way that doesn't involve ubiquitous tracking of our every movement online.

²⁷ Press Release, Seedtag, *Seedtag and Nielsen Research Finds Contextual Targeting Boosts Consumer Interest in Advertising by 32%* (May 11, 2022), <https://press.seedtag.com/seedtag-and-nielsen-research-finds-contextual-targeting-boosts-consumer-interest-in-advertising-by-32>.

Why this is happening: Big Tech is writing the rules

How can all this be happening? Many consumers would likely be shocked to learn just how little their data is protected and that policymakers have largely failed to take meaningful action.

The U.S. still lacks a comprehensive federal privacy law. The few-sector specific laws that do exist were passed in the '80s and '90s, failing to capture how smartphones and constant internet access have given companies entirely new and unprecedented access to individuals' personal information.²⁸ These outdated laws also fail to cover the relatively new phenomenon of online data brokers — arguably the worst actors in this ecosystem — that have only materialized in the last 20 years.

Because Congress has failed to pass a comprehensive privacy law to regulate the technologies that dominate our lives today, state legislatures have tried to fill the void in order to protect their constituents' privacy. Unfortunately for consumers, in states across the country, legislators introducing consumer privacy bills have faced a torrent of industry lobbying vying to weaken protections. Nearly everywhere, they have succeeded. Of the 14 laws states have passed so far, all but California's closely follow a model that was initially drafted by industry giants such as Amazon.²⁹

Of the 14 laws states have passed so far, all but California's closely follow a model that was initially drafted by industry giants such as Amazon.

In 2021, Virginia became the second state in the nation to pass a comprehensive consumer data privacy law. Where California's law — which was passed in 2018 — established some real protections, Virginia's was almost entirely void of meaningful provisions. A notable difference: While California's rules became law in response to a proposed ballot question, Virginia's legislation had been handed to the bill sponsor by an Amazon lobbyist, and it was based on an earlier bill from Washington state that had been modified at the behest of Amazon, Comcast, and Microsoft.³⁰

The Virginia law was weak: Companies could continue collecting whatever data they wanted as long as it was disclosed somewhere in a privacy policy. While consumers could, in theory, request

²⁸ *Grading on a Curve*, *supra* note 4.

²⁹ Jeffrey Datin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, Reuters (Nov. 19, 2021), <https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/>.

³⁰ Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, Protocol (Feb. 19, 2021), <https://www.protocol.com/policy/virginia-maryland-washington-big-tech>; Mark Scott, *How Lobbyists Rewrote Washington State's Privacy Law* (Apr. 2019), <https://www.politico.eu/article/how-lobbyists-rewrote-washington-state-privacy-law-microsoft-amazon-regulation/>.

companies delete their data, they would have to submit requests one at a time to the hundreds — if not thousands — of entities holding their information. Consumers also had no ability to hold companies accountable in court for violating the privacy law meant to protect them. Virginia, in this scorecard, receives an F.

“Virginia is what the lobbyists were asking for,” Walke said. “Making the bill weaker, I understood. Compromise is always necessary. But making it as weak as Virginia is something I have never understood.”

Unfortunately, Virginia became the model lobbyists have pushed many state legislators to match, particularly in red states such as Kentucky and Montana.³¹ In Oklahoma, former state legislator Collin Walke was asked to water down his 2021 Oklahoma Computer Data Privacy Act.

“It was a bipartisan bill,” Walke said in an interview for this report. “People liked it. Before it even hit the House floor it had some 40 co-authors. It passed out of the House 85-11.” When Walke’s bill stalled in the Senate, he knew he was going to have to negotiate some changes. What he didn’t expect, however, was the lobbyist push for a noticeably weaker, Virginia-style bill.

“Virginia is what the lobbyists were asking for,” Walke said. “Making the bill weaker, I understood. Compromise is always necessary. But making it as weak as Virginia is something I have never understood.”

More recently, and particularly in blue states, lobbyists have pivoted to pushing the “Connecticut model” — a bill similar to Virginia with a couple of concessions to consumers.³² Most notably, Connecticut allows consumers to use a browser tool to automatically opt-out of websites collecting data. The law, however, included no ability for a regulator like the Attorney General to specify what exactly the tool should look like, leaving open questions about how well the provision would serve its purpose. In a pattern seen across the country, the law that passed in Connecticut in 2022 ended up weaker than what co-sponsor Sen. Bob Duff had introduced

³¹ Alfred Ng, *How Montana Passed the Strongest Privacy Law Among Red States*, Politico (June 17, 2023), <https://www.politico.com/news/2023/06/17/montana-tech-privacy-law-00101511>; Anna Edgerton, *Tech Lobbyists Don’t Want States to Let You Sue Over Privacy Violations*, Bloomberg (Mar. 20, 2023), <https://www.bloomberg.com/news/articles/2023-03-20/big-tech-lobbyists-are-fighting-strict-data-privacy-laws-state-by-state>.

³² See, e.g., Letter from Tyler Diers, Technet, to Minnesota State Representative Steve Elkins (Jan. 19, 2024), <https://www.lcc.mn.gov/lcdp/meetings/01222024/TechNet-MN-HF2309.pdf> (“TechNet urges you to consider interoperability with existing models as the default position. As you know, it is important that privacy bills across the country provide for interoperability and we appreciate your efforts with other legislators in other states to do so. To date, 12 states have enacted privacy laws that borrow from the Virginia/Connecticut framework. Each new concept or definitional change could result in consumer confusion and significantly increase compliance costs for businesses.”)

previously — notably from his 2020 privacy bill, which included the ability for consumers to sue.³³ Connecticut, in this scorecard, receives a D.

In 2023, the pressure and the strategy remained the same. In Oregon, for example, the State Privacy and Security Coalition — an industry group representing Amazon and Meta, among others — testified at one point that a stronger draft of the Oregon Consumer Privacy Act “still deviate[d] from other state privacy laws” as to “need significant work.”³⁴ In Delaware, the Computer Communications Industry Association — an industry group representing Google and Apple, among others — encouraged in testimony that the state’s bill should “more consistently align with definitions and principles in other existing comprehensive state privacy laws,” pointing to Virginia and Connecticut in particular.³⁵

Industry lobbying has profoundly shaped how states approach consumer privacy, and their efforts have been significant; an investigation by the Markup identified 445 active lobbyists and firms representing Amazon, Meta, Microsoft, Google, Apple, and industry front groups in the 31 states that heard privacy bills in 2021 and 2022. Because of the opacity of state lobbying records, that number is likely an undercount.³⁶

The accelerating passage of industry-preferred bills not only poses a threat for the residents of the states passing ineffectual laws. The more states that coalesce around regulations heavily influenced by the very industries that need to be regulated, the greater the risk of lowering the bar for the effectiveness of a future federal law, which is exactly what industry is hoping for.

³³ Todd Feathers, *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*, The Markup (Apr. 15, 2022), <https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious>.

³⁴ *RE: SB 619 (Comprehensive Privacy)*, written testimony submitted by the State Privacy & Security Coalition (Mar. 6, 2023), <https://olis.oregonlegislature.gov/liz/2023R1/Downloads/PublicTestimonyDocument/61538>.

³⁵ *RE: HB 154 – “the Delaware Data Privacy Act” (Oppose unless Amended)*, written testimony by the Consumer & Communications Industry Association submitted to the Delaware state Senate Banking, Business, Insurance & Technology Committee (June 26, 2023), <https://ccianet.org/library/ccia-comments-on-delaware-hb-154/>.

³⁶ 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>.

The solution: What a strong privacy law looks like

Privacy is a fundamental right, and our laws should reflect that. In this section, we lay out the provisions that states should include in their comprehensive privacy laws to adequately protect consumers online.

Features of strong state-level regulations

Existing state privacy laws simply do not do enough to change business as usual – the collection of endless amounts of personal data that is then used in ways that defy consumers’ expectations. These laws only generally allow individuals to access, correct, and delete personal data about them, or opt-out of certain uses of data – if they have the time and expertise to do so, which is often not the case. On their own, these aren’t real privacy protections.

States should instead impose data minimization obligations on companies that collect and use personal information – taking the burden off individuals to manage their privacy online and instead requiring entities to limit their data collection to better match consumer expectations. They should strictly regulate all uses of sensitive data, including health data, biometrics, and location data. They should establish strong civil rights safeguards online and rein in harmful profiling of consumers. And there needs to be strong enforcement and regulatory powers to ensure the rules are followed.

Data minimization

The excessive data collection and processing that fuels commercial surveillance systems is inconsistent with the expectations of consumers, who reasonably expect that their data will be collected and used for the limited purpose to provide the goods or services that they requested.

Companies should not have a limitless ability to decide how much personal data to collect. Unfortunately, this is what most state laws, including the Virginia and Connecticut “model” laws, allow. By limiting collection to what is reasonably necessary for “the purposes for which such data is processed, *as disclosed to the consumer*,” businesses can collect data for whatever purposes they want, as long as they state that purpose in their privacy policies. 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.

These exploitative practices don’t have to continue. Instead, states can integrate a concept that has long been a pillar of privacy protection: the idea that data collection and use should be limited to what’s necessary in context, known as “data minimization.” To implement this concept, states should integrate the following protections into their privacy laws:

- Data collection, processing, and transfer should be limited to what is reasonably necessary for the product or service an individual requests or for a clearly defined, enumerated permissible purpose. Knowledge or consent should only be relied on in limited circumstances where appropriate.
- Controllers should be required to delete personal data after the data is no longer necessary.
- Very strict limits should be placed on the collection and processing of highly sensitive data, such as biometric, genetic, and precise geolocation data (a “strictly necessary” standard is best).
- Most secondary processing and transfers should be prohibited by default with only narrow exceptions.
- Transfers of sensitive data to third parties (other than to processors) should be prohibited, unless the transfer is strictly necessary and done with affirmative opt-in consent.
- Processors should be explicitly prohibited from engaging in secondary uses and combining data from multiple controllers, and they must adhere to their required contracts with controllers.

Data minimization is essential for both consumers and businesses. Data minimization principles give consumer confidence in using technology, knowing there are rules in place that limit the use of their personal data. And a data minimization rule can provide clear guidance to businesses when designing and implementing their data policies.

Data minimization provisions also increase data security. A data minimization framework means that businesses are collecting less personal data about consumers and promptly deleting data they no longer needed. Ultimately, this means businesses have less data overall, making it less likely that consumer data will be exposed in a data breach.

DATA MINIMIZATION	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Strong data minimization	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Sensitive data collection restriction	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Sensitive data transfer restriction	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Prompt data deletion	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Secondary uses/transfers prohibited	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Universal opt-out signals	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✓	✗	✗

Strong enforcement

Robust enforcement is critical to effective privacy protection. Strong enforcement by state governments via Attorney General authority or the creation of a state privacy agency is a vital piece to include in a strong privacy law.

But while government enforcement is essential, the scope of data collection online is simply too vast for one entity to regulate, particularly state Attorneys General with limited resources. Individuals who use these online services are in the best position to identify privacy issues and bring actions to vindicate their privacy interests. These cases preserve the state's resources, and statutory damages ensure that companies will face real consequences if they violate the law.

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 that controllers have strong financial incentives to comply with state privacy laws. We have seen evidence of this in Illinois,³⁷ 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.³⁸

ENFORCEMENT	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
AG rulemaking	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
AG enforcement authority	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Right to cure *	DISC	SUN	SUN	SUN	MAND	MAND	SUN	SUN	SUN	SUN	MAND	MAND	MAND	MAND
Private right of action	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Injunctive relief	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Statutory damages	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Privacy agency	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

* DISC = Discretionary

SUN = Sunsets

MAND = Mandatory

³⁷ Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), <https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf>.

³⁸ 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>.

Rulemaking authority

California, Colorado, New Jersey, and, to a limited extent, New Hampshire have all included rulemaking authority in their state privacy laws. Rulemaking authority is critical in providing guidance to businesses on compliance with the law and ensuring the law can keep pace with technology.

Civil rights protections

Most state privacy laws attempt to prevent discrimination online by prohibiting the processing of personal data in ways that violate state and federal anti-discrimination laws. However, existing civil rights laws contain significant gaps in coverage and do not apply to disparate impact.³⁹ These issues make existing laws insufficient to ensure all people are protected from discrimination online. Therefore, states should instead include language that prohibits controllers and processors from collecting, processing, or transferring 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.”

Transparency and assessing high-risk data practices

Companies collecting and using personal data should be required to assess their systems that present risks of harm to consumers. Many states have included requirements to conduct data protection impact assessments or other similar risk assessments, which can help with meaningful oversight, if done right.

To be meaningful, these assessments should include documentation of what personal data is being collected, why that personal data is being collected, whether and how that personal data is being used and transferred/sold, what risks there are to consumers from use of their personal data, potential benefits to the consumer from the collection and use of their personal data, an explanation of why these benefits outweigh the risks, how these risks are being mitigated, and identification of alternatives to profiling and why these alternatives were rejected.

Risk assessments should be required within a reasonable time of the law going into effect and should cover processing activity that began before the law’s enactment but is ongoing. Controllers should be required to do these assessments on a regular basis and update them upon any material changes.

³⁹ See Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. on Consumer Protection & Comm. of the H. Comm. on Energy & Comm., 117th Cong. (2022) (testimony of David Brody, Lawyer’s Comm. for Civil Rights Under Law), <https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-Wstate-BrodyD-20220614.pdf>.

Critically, a version of this risk assessment (or, at minimum, a summary of the risk assessment) must be accessible to the public. Without this requirement, these assessments can simply become internal box-checking exercises.⁴⁰

TRANSPARENCY AND DATA SECURITY	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Data security requirement	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Privacy policy standards	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Notice of policy changes	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
Accessible privacy policies	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Impact assessments	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Reasonable time	✗	✓	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗
Regularly reviewed	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Publicly available	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Meaningful individual rights

Every state privacy law reviewed in this report contains some form of individual rights. These rights typically include the right to access and correct inaccuracies in your personal data and to request its deletion. These rights alone are not enough to protect privacy, but they are an important component of any comprehensive privacy bill.

There are four key protections within individual rights that states should integrate to make those rights meaningful:

- Require companies to honor universal opt-out signals. Many states have included this requirement in their privacy laws.
- Deletion rights should apply to any data connected to a consumer, not solely data collected from the consumer. The language from Connecticut’s law can be used (“delete personal data provided by, or obtained about, the consumer”).
- Oregon and Delaware have added the right to obtain information about third parties to whom a company has disclosed your personal data.
- Authorized agents should be permitted to execute all individual rights, not solely opt-out rights. The California Consumer Privacy Act contains this right, and researchers at

⁴⁰ See generally Ari Ezra Waldman, *Industry Unbound* (2021) (demonstrating that many privacy impact assessments conducted under GDPR have become little more than checkbox forms).

Consumer Reports have found that it helps make consumers' individual rights more meaningful.⁴¹

CONSUMER RIGHTS	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Right to access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Right to correct	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Right to delete	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Authorized agent can exercise	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Profiling opt-out	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Bans discrimination for using rights	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗
Protection for minors' data	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗

Banning manipulative design and unfair marketing

Individuals should not be forced to trade basic privacy rights to obtain services. Such provisions undermine the purpose of privacy law: to ensure baseline protections for consumers.

There are a few key protections states should include in their privacy laws to prevent unfair business practices. First, the use of data collected for loyalty programs should be limited to what is functionally necessary to operate the loyalty program. Companies should not be able to collect consumers' personal data with the promise of a discount or loyalty program perk and then turn around and sell that data to other companies to make a profit. Companies do not need to sell personal data to scores of third parties in order to operate a loyalty program. The use of personal data collected for such programs for cross-site targeted advertising and sale to third parties should be prohibited.

Second, states should prohibit discrimination against consumers who exercise their privacy rights. Consumers should not be charged a higher price for goods if they have opted out of targeted advertising.

⁴¹ Kaveh Waddell, *How 'Authorized Agents' Plan to Make It Easier to Delete Your Online Data*, Consumer Reports (Mar. 21, 2022), <https://www.consumerreports.org/electronics/privacy/authorized-agents-plan-to-make-it-easier-to-delete-your-data-a8655835448/>.

Third, “dark patterns,” or manipulative design meant to subvert consumer choice, should be prohibited in both the definition of consent and in the provisions granting consumer rights. Design choices that purposely deter consumers from exercising their privacy rights undermine the very purpose of a privacy law – to empower consumers.

UNFAIR BUSINESS PRACTICES	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Civil rights protections	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Loyalty program data limits	✓	X	X	X	X	X	X	X	X	X	X	X	X	X
Prohibits dark patterns	✓	✓	✓	✓	X	X	✓	✓	✓	✓	X	✓	X	X

Importance of strong definitions

Definitions can make or break a privacy law. Some key definitions EPIC and U.S. PIRG analyzed in our review are:

Personal data: Personal data should be defined as information that is linked to or could be linked to a person, household, or device and should include inferences/derived data. Most states fail to include inferences or derived data. Sensitive inferences about us are often derived from publicly available data, and those should be covered in the definition of personal data. Pseudonymous data should not be exempted from the definition (or any portion of a privacy bill), as it includes identifiers such as IP addresses and device IDs that can be easily reassociated with an individual.

Controllers/covered entities: Ideally, state privacy laws should include all entities that handle personal data. Any threshold 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 sensitive personal data. Any carveouts for entities covered by existing privacy laws should be limited to the specific information protected by existing privacy laws, not the entity (or their affiliates) as a whole. For example, many states exempt entities covered by the Gramm-Leach-Bliley Act (GLBA). GLBA is weak legislation that primarily requires financial institutions to offer an opt out of disclosure to third parties and does not provide even basic access or deletion rights. It is inappropriate to exempt entire entities from coverage of a comprehensive privacy law simply because some of the data they collect is covered by a federal law with limited privacy protections.

Sale/share/transfer: Most privacy laws modeled on Virginia or Connecticut define “sale of personal data” so narrowly that it fails to cover many harmful data uses that consumers should be protected from. The definition should be broadened to include making data available for any commercial purpose, not only for monetary or other valuable consideration. Many unexpected

secondary uses of consumers’ personal data happen when access to their personal data is sold for the purposes for targeting or profiling, but because the personal data itself is not exchanged in these instances, these uses fall outside of many definitions. This was one of the primary reasons that California’s privacy law was updated via ballot question in 2020.

Profiling: Any definition of profiling or automated decision-making system should focus on the function of the system (aiding or replacing human decision-making) and cover both sophisticated AI models and simpler algorithms and automated processes. The definition in the Connecticut law is a good model definition.

Targeted advertising: The definition of targeted advertising should match consumer expectations of what that term means. States should be careful not to incorporate loopholes into this definition that would fail to cover companies with massive troves of consumer data, such as Google and Meta, using that data to serve targeted ads – to do so would defeat the entire purpose of a targeted advertising opt-out.

Biometric data: Most state laws define biometric data too narrowly, requiring that the biometric data “is used” to identify an individual. Biometric data should include information that could be used to confirm the unique identification of a consumer rather than limited to data that is affirmatively used to do so. A fingerprint or faceprint is very sensitive data, whether it has been used to identify the individual yet or not.

STRONG KEY DEFINITIONS	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Personal/covered data	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
No pseudonymous exemption	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✗	✓	✗
Biometric data	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗
Covered entity/controller	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓
Narrow carveouts	✓	✓	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗
Sell/share	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗
Profiling	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Targeted advertising	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Grading on a curve: How state laws fail to protect consumers' privacy and security

We evaluated each of the 14 state comprehensive consumer privacy laws that have been passed as of February 1, 2024.

We graded the state laws based on the provisions explained above — elements that would be found in a privacy law that provides meaningful protections for consumers. The most important aspects of a protective privacy law — data minimization requirements, strong Attorney General enforcement and rulemaking, and a private right of action — earned the most points. Our full scorecard, including a breakdown of how points were allocated, can be found in Appendix B.

Of the 14 laws, nearly half received a failing grade. None received an A.

California: an advancing “B” state

California

California Consumer Privacy Act

Date law took effect: January 1, 2020

Score: 69/100

B+

In 2018, California passed the nation's first comprehensive privacy law, the California Consumer Privacy Act. This law was amended in 2020 when voters passed a ballot initiative known as the California Privacy Rights Act, which strengthened the 2018 law. As it stands today, California's privacy law is the strongest in the nation, though it does lack many critical consumer protections.

California recently passed the DELETE Act,⁴² which would allow California residents to make one deletion request that all data brokers in the state must comply with. Under the text of the CCPA and corresponding regulations, the right to delete applies only to personal information provided by the consumer (rather than personal data obtained about the consumer). However, the recently enacted DELETE Act, which will be enforced by the California Privacy Protection Agency, covers the deletion of all personal data about a consumer who submits a request. Based on these protections, we awarded California the point for the right to delete.

Privacy-protective provisions:

- Established an independent privacy agency with rulemaking authority
- Prohibits the use of financial incentive practices (such as loyalty programs) that are unjust, unreasonable, coercive, or usurious in nature
- Limited carveouts only for data regulated by other privacy laws (rather than entity-level)
- No exemption for pseudonymous data
- Privacy protections cannot be weakened by the Legislature

Missing provisions:

- Heightened protections for sensitive data by default
- Clear limits on cross-site browser tracking
- Detailed restrictions in statute's data minimization framework
- Private right of action for violations of the law outside of those that result in data breaches

Possible amendments/rulemaking:

- Strengthen the definition of biometric data.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Continue using rulemaking authority to protect consumers' data and privacy rights.

⁴² Cal. Civ. Code § 1798.99.86 (West 2023).

The middling “C” states

Colorado

Colorado Privacy Act

Date law took effect: July 1, 2023

Score: 41/100



When Colorado enacted the Colorado Privacy Act in 2021, the state included strong rulemaking authority for the Attorney General for purposes of implementing the law. This has allowed the Attorney General to provide guidance to both businesses and consumers on the more technical aspects of the bill, such as what constitutes a dark pattern and how to implement a global opt-out mechanism. In July 2024, Colorado residents will be able to download and use the Global Privacy Control tool to automatically broadcast to websites that they don't want their data collected. (You can download that [here](#), and see CoPIRG's consumer guide [here](#).)

Privacy-protective provisions:

- Attorney general has rulemaking authority
- Requires controllers to honor global opt-out signals
- Limited carveouts only for data regulated by other privacy laws rather than broad, entity-level exemptions
- Robust prohibitions on dark patterns/deceptive design

Missing provisions:

- No private right of action
- Limited data minimization requirements

Possible amendments/rulemaking:

- Strengthen the definition of sell/share.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.
- Prohibit price discrimination against consumers who exercise their privacy rights.
- Continue using rulemaking authority to protect consumers' personal data and privacy rights.

New Jersey



Senate Bill 332 (name pending)

Date law will take effect: January 16, 2025

Score: 37/100

New Jersey is one of the most recent states to pass a privacy law. The governor signed it into law on Jan. 16, 2024.

Privacy-protective provisions:

- Attorney general has rulemaking authority
- No exemption for pseudonymous data

Missing provisions:

- No data minimization requirements
- No private right of action

Possible amendments/rulemaking:

- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.
- Strengthen definitions of personal data and biometric data.
- Change carveout for GLBA from all financial institutions covered by the law to only the data that is regulated by the law.
- Use rulemaking authority to its fullest extent to protect consumers' personal data and privacy rights.

Oregon

Oregon Consumer Privacy Act

Date law will take effect: July 1, 2024

Score: 31/100



Passed in June 2023, the Oregon Consumer Privacy Act was the result of a working group led by the Oregon Attorney General's office. Despite this, it still followed the Connecticut model, though Oregon did add some important protections – including minimizing the number of entities who were exempt from the law.

Privacy-protective provisions:

- No exemption for pseudonymous data
- Limited carveouts only for data regulated by other privacy laws rather than broad, entity-level exemptions
- Broad definition of sensitive data that includes “status as transgender or nonbinary” and “status as a victim of a crime”
- Adds a consumer right to obtain a specific list of third parties to which the controller has disclosed either that consumer's personal data or personal data generally

Missing provisions:

- No Attorney General rulemaking authority
- No private right of action
- No data minimization requirements

Possible amendments:

- Strengthen the definition of sell/share.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.

Delaware

Delaware Personal Data Privacy Act

Date law will take effect: January 1, 2025

Score: 30/100



The Delaware governor signed the Personal Data Privacy Act into law on Sept. 11, 2023. State lawmakers heard the same message from Big Tech that industry has repeated since passage of the Virginia "model": Delaware's bill should "more consistently align with definitions and principles in other existing comprehensive state privacy laws," pointing to Virginia and Connecticut.⁴³

Privacy-protective provisions:

- Bans targeted advertising to minors under 18 years old
- Broad definition of sensitive data that includes "status as pregnant" and "status as transgender or nonbinary"
- Gives consumer the right to obtain a list of the categories of third parties with whom the controller has shared the consumer's own personal data

Missing provisions:

- No Attorney General rulemaking authority
- No private right of action
- No data minimization requirements

Possible amendments:

- Strengthen definitions of personal data, sell/share, and biometric data.
- Change carveout for GLBA from all financial institutions covered by the law to only the data that is regulated by the law.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.

⁴³ The Computer Communications Industry Association (CCIA) — an industry group representing Google and Apple, among others — testified at hearings about the Delaware law. *RE: HB 154 – "the Delaware Data Privacy Act" (Oppose unless Amended)*, written testimony by the Consumer & Communications Industry Association submitted to the Delaware state Senate Banking, Business, Insurance & Technology Committee (June 26, 2023) <https://ccianet.org/library/ccia-comments-on-delaware-hb-154/>.

Lagging “D” states

Connecticut



Connecticut Data Privacy Act
Date law took effect: July 1, 2023
Score 24/100

Connecticut’s Data Privacy Act was first introduced in 2019 and originally included strong provisions such as a private right of action. The bill, however, was whittled down over time, making it more similar to Virginia’s failing law. In 2022, Connecticut’s bill was passed with a few additional provisions — such as requirements to honor global opt-out signals — making it a little stronger than Virginia. This bill has now become a favored piece of template legislation for lobbyists, particularly in bluer states.

A year after its original passage, Connecticut passed legislation amending the law to include heightened protections for kids and teens online and adding a category of sensitive data for “consumer health data.” The “Connecticut model” pushed by industry in other states does not include these updates.

Privacy-protective provisions:

- Requires controllers to honor global opt-out signals (though requirement that controllers “accurately determine” residency should be revised)
- Enhanced protections for minors under 18, including a ban on targeted advertising (Note: these additional protections are part of the 2023 amendments, not the original “Connecticut model” being pushed by industry.)

Missing provisions:

- No data minimization requirements
- No private right of action
- No Attorney General rulemaking authority

Possible amendments:

- Strengthen definitions of personal data, sell/share, and biometric data.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Change carveouts for existing privacy laws to be data-level exemptions rather than entity-level exemptions.
- Require companies to make impact assessments (or a summary) available to the public.

New Hampshire



Senate Bill 255 (*name pending*)

Date law will take effect: January 1, 2025

Score: 22/100

New Hampshire is the most recent comprehensive consumer privacy law to pass. The bill passed out of the Legislature on Jan. 18, 2024 and is awaiting the governor's signature.

Privacy-protective provisions:

- Some Attorney General rulemaking authority (though limited)

Missing provisions:

- No data minimization requirements
- No private right of action

Possible amendments:

- Strengthen definitions of personal data, sell/share, and biometric data.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.
- Change carveouts for existing privacy laws to be data-level exemptions rather than entity-level exemptions.
- Expand Attorney General rulemaking authority to better protect consumers' personal data and privacy rights.

Montana



Consumer Data Privacy Act

Date law will take effect: October 1, 2024

Score: 20/100

Before Republican Sen. Daniel Zolnikov introduced the Consumer Data Privacy Act, a tech lobbyist told him the Connecticut model was too difficult for industry to comply with and that it would be better to introduce something closer to the weaker Virginia model. According to Politico, after Zolnikov heard the same lobbyist testify in Maryland — a blue state — that industry would be happy with a Connecticut model, he strengthened his bill.

Zolnikov has expressed frustration with being pushed to pass a weaker bill in Montana than in blue state counterparts. “I’m not an idiot,” Zolnikov said in an interview with Politico after the passage of his bill, directing his comments at the lobbyist. “And you treating us in Montana like a bunch of rural backwoods folks is quite an insult.”⁴⁴

Privacy-protective provisions:

- Requires controllers to honor global opt-out signals (though requirement that controllers “accurately determine” residency should be revised)
- Though it includes a right to cure for Attorney General enforcement, that requirement sunsets 18 months after enactment.

Missing provisions:

- No data minimization requirements
- No private right of action
- No Attorney General rulemaking authority

Possible amendments:

- Strengthen definitions of personal data, sell/share, and biometric data.
- Change carveouts for existing privacy laws to be data-level exemptions rather than entity-level exemptions.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.

⁴⁴ Ng, *supra* note 31.

The failing “F” states

Below are the 6 states that received an F: Texas, Virginia, Indiana, Tennessee, Utah, and Iowa. These laws all scored less than 20%.

The first of these states to pass a privacy law was Virginia. Amazon targeted business-friendly Virginia Sen. David Marsden and handed him ready-to-go legislation that would allow Big Tech’s business model to continue uninterrupted.⁴⁵ That bill became Virginia law in 2021 and quickly became the model pushed by the tech industry across the country.



Utah took the Virginia model and made it even more business-friendly, changing the law so that it only covered businesses making more than \$25 million. The state ultimately passed its failing law in March 2022.

Iowa, Indiana, Tennessee, and Texas all passed versions of this “Virginia model” throughout the spring and summer of 2023.

These laws’ dismal — and strikingly similar — scores reflect their weak, business-friendly language and lack of meaningful consumer protections. These state laws represent the first industry success stories, where the law written by Amazon, passed by Virginia, and copied by these states was enacted.

Texas

Texas Data Privacy and Security Act
Date law will take effect: July 1, 2024
Score: 16/100

Tennessee

Tennessee Information Protection Act
Date law will take effect: July 1, 2025
Score: 6/100

Virginia

Consumer Data Protection Act
Date law took effect: January 1, 2023
Score: 11/100

Utah

Utah Consumer Privacy Act
Date law took effect: December 31, 2023
Score: 6/100

Indiana

Consumer Data Protection
Date law will take effect: January 1, 2026
Score: 11/100

Iowa

Iowa Data Privacy Act
Date law will take effect: January 1, 2025
Score: 4/100

⁴⁵ Datin, Kirkham & Kalra, *supra* note 29.

None of these laws provides meaningful privacy protections to consumers.

Without a data minimization framework, these laws allow companies to continue their business as usual — collecting as much personal data as they can so that they can target individual consumers with incessant targeted advertisements, sell it to massive data brokers to aggregate and create profiles of consumers, and make enormous profits off of the thriving advertising ecosystem.

Without a requirement that businesses honor universal opt-out signals, consumers are forced to play whack-a-mole with companies, telling businesses one by one not to sell their data or target them with ads.

Without a private right of action, consumers have no way to protect the minimal privacy rights these laws do provide.

At best, these laws enshrine the status quo. At worst, they allow Big Tech to say they care about privacy while at the same time lobbying in states all across the country to strip away consumer protections and weaken privacy laws.

Illinois' opportunity to lead the class

Illinois gets an “incomplete,” as it has yet to pass a comprehensive consumer privacy law. However, it has the opportunity to lead the class.

Illinois Data Privacy and Protection Act (HB3385, Rep. Abdelnasser Rashid)

Score: 99/100

A

This bill gets a near-perfect score and, if passed as is, would be the strongest comprehensive privacy law in the country. Because of its data minimization framework, private right of action, strong enforcement and rulemaking provisions, and limited exemptions, this bill would protect Illinois residents' personal data better than any privacy law passed so far.

Illinois is no stranger to strong privacy protections. Its Biometric Information Privacy Act is the strongest biometric privacy law in the nation, and its inclusion of a private right of action has led to better outcomes for consumers.

Appendix A: Methodology

Which laws were evaluated?

We evaluated only state privacy laws that are comprehensive in scope and excluded more narrow laws focusing on one specific area of privacy. For example, laws such as Washington’s My Health, My Data⁴⁶ or Illinois’s Biometric Information Privacy Act⁴⁷ were not included in this report because they cover only a narrow slice of consumer data. While sectoral privacy laws like these do protect some types of information, this report focuses on state laws that claim to provide broad privacy protections for consumers across all types of personal data.

The states with comprehensive privacy laws that we evaluated are: California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia. We did not include the Florida Digital Bill of Rights as a comprehensive privacy law because of its limited applicability to only businesses with more than \$1 billion in revenue.⁴⁸

Funding

Even the most well-written comprehensive privacy law can only be effective if it allocates adequate funding for the Attorney General’s office to conduct rulemaking and enforce the law. Without funding to enforce the law, even laws that meet the above criteria are meaningless. Because of how vital adequate funding is, we included it on the scorecard as a key provision of a strong privacy law.

However, because states have different mechanisms for allocating funding (in separate appropriations bills, for example), we did not evaluate or assign any points to any state for this criteria. Funding is included in the scorecard to emphasize its importance, but it did not play a role in the grade any state received due to the difficulty in assessing this factor.

States with rulemaking authority

The laws in California, Colorado, and New Jersey all granted rulemaking authority to the state’s Attorney General. In scoring these laws, we awarded full points if the actual statutory text of the California and Colorado laws met our rubric criteria. We awarded partial points if those states’ regulations fulfilled our rubric criteria.

Because the New Jersey bill was only signed into law a few weeks before this report’s publication, the state does not yet have any regulations. Thus, New Jersey’s score was based only on the text of its statute.

⁴⁶ Wash. Rev. Code Ann. § 19.373.005 (West, Westlaw Edge through 2023 Reg. and First Special Sessions).

⁴⁷ 740 ILCS 14/1 (West 2008).

⁴⁸ § 501.701 Fla. Stat. (2023).

New Hampshire also granted extremely limited rulemaking authority to the Secretary of State. Based on this, New Hampshire received partial points in the rulemaking category, and given that the law was only signed into law a few weeks before this report's publication, there are no regulations yet to score.

Interactions with other state laws

There may be other state laws that could be relevant to some of the criteria we identified. For example, states may have anti-discrimination laws or data security laws that are separate from the comprehensive privacy laws we evaluated.

For the grading, we only generally considered the text of the specific statute we were evaluating as well as any corresponding regulations, when applicable. Because we did not have the ability to look at every law within each state that we graded, the grades are based solely on the text of the state's privacy law.

Appendix B: Grading criteria

STRONG KEY DEFINITIONS (6)

- **Personal data** definition should cover information that is linked or could be linked to a person, household, or device and should include inferences/derived data. (1)
 - *Exemption for pseudonymous data (-3 if present)*
 - *Or, if exemption for pseudonymous data applies only to consumers' rights to access, correct, delete (-1 if present)*
- **Controllers/covered entities** definition should include all entities that handle personal data, and requirements should be defined based on how much data entities process rather than their revenue. (1)
 - *Broad, entity-level carveouts for entities covered by existing privacy laws rather than narrow, data-level carveouts (-5 if present)*
 - *Or, if only some carveouts are entity-level while others are data-level (-3/-2 if present, depending on scope)*
- **Sell/share** definition should include disclosing, making available, transferring, or otherwise communicating personal data to a third party for monetary or other valuable consideration or otherwise for a commercial purpose. (1)
- **Profiling** definition should be defined as the use of an automated processing or decision-making system to process personal data to evaluate, infer, or predict information about an individual. (1)
- **Targeted advertising** definition should cover the targeting of advertisements to a consumer based on the consumer's interactions with one or more businesses, distinctly branded websites, applications, or services other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. (1)
- **Biometric data** definition should include information that can be used to confirm the unique identification of a consumer rather than information that is affirmatively used to do so. (1)

ENFORCEMENT AND REGULATORY BODIES (22)

- Strong rulemaking authority (8)
- Strong enforcement authority in the Attorney General or independent privacy agency (8)
 - No mandatory right to cure (6)
 - Right to cure at the discretion of the Attorney General (4)
 - Right to cure that sunsets (3)
 - Mandatory right to cure with no sunset (0)
- Establishes an independent privacy agency (+10)
- Appropriates adequate funding for rulemaking and enforcement*

ENFORCEMENT VIA PRIVATE RIGHT OF ACTION (14)

- Private right of action (7)
 - Injunctive relief available (4)
 - Statutory damages available (3)

DATA CONTROLLER/PROCESSOR OBLIGATIONS

Data Minimization (14)

- Data collection, processing, and transfer is limited to what is reasonably necessary for the product or service the consumer requested or a clearly defined, enumerated purpose (7)
- Data must be deleted when no longer necessary for original purpose (3)
- Collection and processing of sensitive data must be strictly necessary (4)
*Knowledge and consent did not receive any points.

Use and Disclosure Limitations (12)

- Prohibits most secondary processing and transfers by default (8)
 - Or, covered entities are required to honor universal opt-out signals (3)
 - Or, if covered entities are required to honor universal opt-out signals, but there are unnecessary authentication requirements (2)
- Transferring sensitive data to third parties is prohibited (unless strictly necessary and done with opt-in consent) (4)
- *Targeted advertising is banned (+5)*

Data Security Requirements (2)

- Controllers have a duty of care to protect data (2)

Transparency about Business Practices (-4 if not present)

- Controllers and processors must have privacy policies that meet certain minimum standards (-2 if not present)
- Consumers must be notified of material changes and given the opportunity to withdraw consent (-1 if not present)
- Privacy policies must be easily accessible to all consumers (-1 if not present)

Enhanced Protections for Children and Teens (+3)

- *Targeted advertising to minors is banned (+3)*
 - *Or, required opt-in consent for targeted advertising to teens (already required for children under 13 by COPPA) (+1)*

PROHIBITS DISCRIMINATORY USES OF DATA (5)

- Bans processing of data in a manner that discriminates, in treatment or effect, or otherwise makes unavailable the equal enjoyment of goods or services on the basis of a protected class (5)

**Provisions that only prohibit discrimination that violates state or federal law did not receive points.*

PROFILING AND IMPACT ASSESSMENTS (12)

- Requires controllers to conduct impact assessments that meet a minimum standard on use of personal data for profiling or other uses that present a risk of harm (4)
 - Impact assessments should be done within a reasonable time (1)
 - Impact assessments should be updated regularly (1)
 - Impact assessments (or a summary) should be made publicly available (4)
- Consumers have the right to opt-out of profiling (2)
- *Especially harmful uses of AI are prohibited (+5)*

INDIVIDUAL RIGHTS (6)

- Access (2)
- Accuracy and correction (2)
- Deletion (must include data obtained about a consumer, not just collected from the consumer) (2)

**One point was awarded for the existence of each right, and one point was awarded if authorized agents are allowed to exercise that right on behalf of a consumer.*

BANS MANIPULATIVE DESIGN AND UNFAIR MARKETING PRACTICES (7)

- Bans price discrimination against consumers who exercise individual rights, including the right to opt-out of targeted advertising (2)
- Limits use of loyalty program data to what is necessary to operate program (3)
- Bans dark patterns/deceptive design (2)
 - Or, if only dark patterns in obtaining consent were banned (1)