

The State of Privacy

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

**Electronic Privacy Information Center (EPIC)
U.S. PIRG Education Fund
January 2025**

The State of Privacy:

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

Written by:

Caitriona Fitzgerald

Kara Williams

Electronic Privacy Information Center (EPIC)

R.J. Cross

Ellen Hengesbach

U.S. PIRG Education Fund

January 2025

epic.org

ELECTRONIC
PRIVACY
INFORMATION
CENTER

U.S. PIRG
Education Fund

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.

U.S. 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 U.S. 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 U.S. 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, U.S. 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 U.S. PIRG Education Fund, please visit www.pirg.org/edfund.

Table of contents

Executive summary.....	4
Introduction.....	7
The problem: Without rules, data abuse runs rampant.....	9
Many companies collect and use data in surprising — and risky — ways.....	9
Unchecked data collection puts consumers’ security at risk, turbocharges targeted scams, and increases the odds of identity theft.....	11
Using data to profile consumers often leads to discriminatory outcomes.....	12
Current data practices can inundate consumers with annoying — and even harmful — targeted advertising.....	13
Despite these urgent harms, Congress has failed to pass federal privacy legislation.....	15
Why this is happening: Big Tech has been allowed to write its own rules.....	15
How the tech industry’s favored privacy bill became the standard across the states.....	16
‘Big Tech has a playbook’.....	18
State lawmakers are increasingly championing meaningful privacy protections instead of settling for the industry model.....	21
The solution: What a strong privacy law looks like.....	23
Features of strong state-level regulations.....	23
Data minimization.....	24
Strong enforcement.....	26
Rulemaking authority.....	27
Civil rights protections.....	27
Transparency and assessing high-risk data practices.....	28
Meaningful individual rights.....	29
Banning manipulative design and unfair marketing.....	30
Importance of strong definitions.....	31
Grading on a curve: How state laws fail to protect consumers’ privacy and security.....	34
Advancing “B” states.....	35
California.....	35
Maryland.....	36
The middling “C” states Colorado.....	37
Colorado.....	37
New Jersey.....	38
Minnesota.....	39
Oregon.....	40
Delaware.....	41
Lagging “D” states.....	42
Connecticut.....	42
New Hampshire.....	43
Montana.....	44
The failing “F” states.....	45

Rhode Island.....	45
Texas.....	45
Kentucky.....	46
Nebraska.....	46
Virginia.....	46
Indiana.....	45
Tennessee.....	45
Utah.....	46
Iowa.....	46
Moving forward: It’s not too late to set a stronger standard.....	47
Appendix A: Methodology.....	49
Appendix B: Grading criteria.....	51
Appendix C: State grading tables.....	54

Executive summary

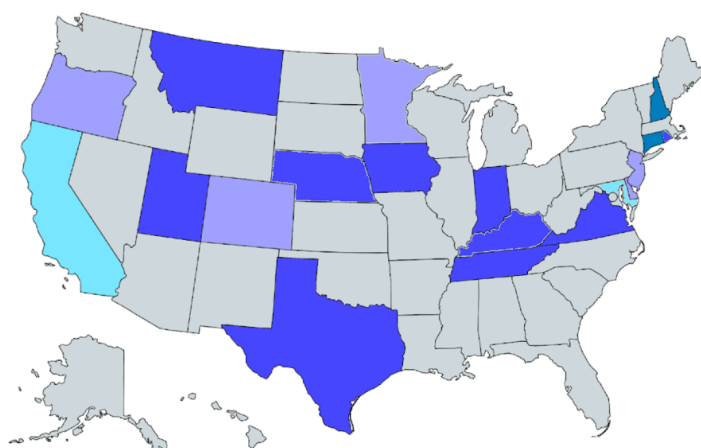
Today, we live much of our lives online. Screens often mediate how we work, learn, and play, and these screens have companies on the other side gathering data about us. Often, these practices are out of line with what consumers expect, putting consumer security and privacy at risk.

The more data companies collect about us, the more our data is at risk. When companies hold your data, the greater the odds it will be exposed in a breach or a hack and end up in the hands of identity thieves, scammers, or shadowy companies known as data brokers that buy and sell a huge amount of data about Americans. The unregulated online advertising and data broker market can result in turbocharged scams, discrimination, and invasive targeted ads.

In our evaluation of the 19 states that have passed consumer privacy legislation, nearly half received failing grades, and none received an A.

Despite the increasing visibility of unchecked data collection and its attendant harms, and data collection and sales being a multi-billion-dollar industry propagated by some of the most powerful companies in the world, Congress has failed to pass a comprehensive federal privacy law. To fill this void, an increasing number of states have passed laws that aim to protect people's privacy and security. However, these laws largely fail to adequately protect consumers. In our evaluation of the 19 states that have passed comprehensive consumer privacy legislation, nearly half received failing grades, and none received an A.

State Consumer Privacy Grades



epic.org

ELECTRONIC
PRIVACY
INFORMATION
CENTER

U.S. PIRG
Education Fund

State	Grade	Score
California	B+	69
Maryland	B-	52
Colorado	C+	42
New Jersey	C	36
Minnesota	C-	34
Oregon	C-	31
Delaware	C-	30
Connecticut	D	22
New Hampshire	D	22
Montana	D	20
Rhode Island	F	18
Texas	F	15
Kentucky	F	14
Nebraska	F	14
Indiana	F	11
Virginia	F	11
Utah	F	6
Tennessee	F	6
Iowa	F	4

Weak, industry-friendly laws allow companies to continue collecting consumers' personal data 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 19 laws states have passed so far, the vast majority closely follow a model that was initially drafted by industry giants such as Amazon. In an analysis of lobbying records in 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.

Laws should not be written by the companies they regulate. Allowing Big Tech to shape our privacy rules enables 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.

A strong comprehensive consumer privacy law would:

- impose meaningful 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, and the tide is beginning to turn. Lawmakers are not satisfied with weak bills that protect Big Tech's harmful business practices more than their constituents' privacy. And after watching another failed congressional attempt to pass a national privacy law, state legislators realize this urgent issue is up to them to solve.

In 2024, states including Illinois, Maine, Massachusetts, and Vermont considered strong legislation that would force changes to the abusive data practices driving commercial surveillance and online discrimination while allowing businesses to continue to innovate. Maryland passed a landmark state privacy law with strong data minimization provisions and a ban on the sale of sensitive data. We can have a strong technology sector while also protecting personal privacy. And states can lead the way.

Introduction

In today's world, we live so much of our life 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 companies collect 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 invisible economy has materialized, made up of thousands of secretive data companies trafficking 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 expect to get.¹ For example, the Kroger grocery chain has embraced mass data collection and sale as an alternative source of profit by opening two new business streams — advertising and data operations — that the company predicts could generate \$1 billion per year in profits for its investors.²

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.³ 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.⁴

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

Despite the public's growing unease, meaningful consumer protections are largely nonexistent. The U.S. still lacks a comprehensive federal privacy law. The existing sector-specific laws — such as the Electronic Communications Privacy Act and the Health Insurance Portability and

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/>.

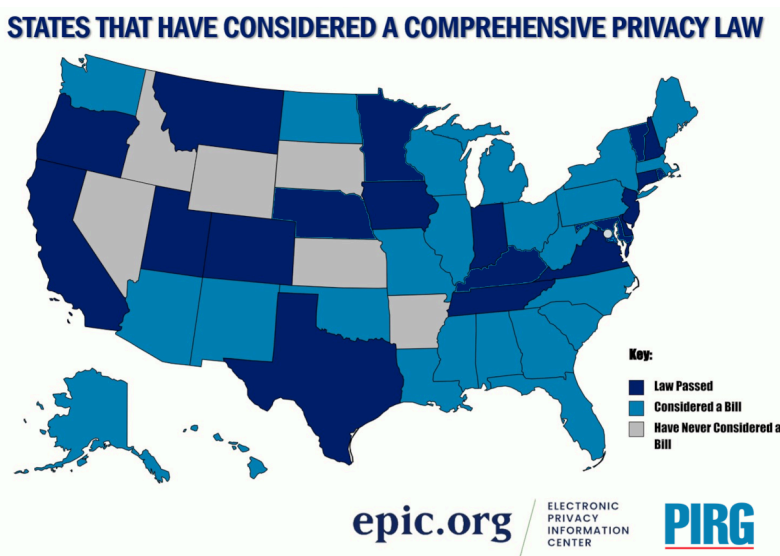
² Jon Keegan, *Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You*, The Markup (Feb. 16, 2023), <https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you>.

³ 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/>.

⁴ *Id.*

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.⁵

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 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.⁶



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.⁷ As of December 2024, 19 states have passed comprehensive privacy laws.⁸

⁵ 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>.

⁶ *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/>.

⁷ Based on an analysis of IAPP trackers. See *The Growth of State Privacy Legislation*, IAPP (Sept. 2022), https://iapp.org/media/pdf/resource_center/growth_of_state_privacy_infographic.pdf and *US State Privacy Legislation Tracker 2024*, IAPP, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

⁸ Andrew Folks, *US State Privacy Legislation Tracker*, IAPP (Jan. 19, 2024), <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.

Unfortunately, the vast majority of these statutes fail to give consumers meaningful protections. 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 rules allow Big Tech to continue amassing and abusing our personal data for its own benefit and profit.

In this report, EPIC and U.S. PIRG Education Fund have come together to shed light on the alarming trend of weak state privacy laws and how to change course.

The problem: Without rules, data abuse runs rampant

Without meaningful limits on the collection and use of personal data, companies are incentivized to collect as much data about consumers as possible and 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.⁹ Another example comes from a 2023 Mozilla Foundation investigation, which found that 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.¹⁰

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

⁹ 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>.

¹⁰ 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/>.

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.’”¹¹ A 2022 study by Human Rights Watch found that educational apps and websites used by schools were harvesting the data of millions of schoolchildren, sending children’s information to data brokers and advertising technology companies while they learned.¹² An investigation by the *New York Times* this year found that some automakers, including G.M., were collecting people’s driving data and selling it to data brokers such as LexisNexis, that were, in turn, selling it to insurance companies and being used to raise people’s insurance rates — often without people knowing.¹³

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 don’t intend to interact with an online service at all. Activities like credit card purchases¹⁴ and even physical movements¹⁵ 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, exposes the average American’s data 747 times per day.¹⁶

These trackers collect millions of data points each day that are sold or transferred to data brokers, who 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.¹⁷ They build profiles on us to facilitate the systems that 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’ insurance prices, or to deny people jobs or housing.

¹¹ 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>.

¹² 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/>.

¹³ Kashmir Hill, *Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies*, New York Times (March 11 2024), <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>

¹⁴ R.J. Cross, *How Mastercard Sells its ‘Gold Mine’ of Transaction Data* (Sept. 2023), <https://pirg.org/edfund/resources/how-mastercard-sells-data/>.

¹⁵ 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>.

¹⁶ 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>.

¹⁷ EPIC, *Data Brokers*, <https://epic.org/issues/consumer-privacy/data-brokers/>.

This ubiquitous tracking of everything we do online, and the entities that aggregate and monetize it, threatens consumers' privacy, autonomy, and security – and it shouldn't be allowed to continue unregulated. The rules we suggest in this report limit data collection and use to what is *reasonably necessary* for the product or service you're requesting, which would force companies to better align their data practices with consumers' expectations. This rule would limit companies from tracking consumers' behavior across the web and stop the flow of endless amounts of personal data to 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 dramatically increases the chances that our personal information will be breached. Once exposed, hackers and other bad actors sell this breached information, including 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 financial accounts can more easily be compromised when hackers access the vast tracking data that online companies generate.

The widespread adoption of the internet and the rise of tracking technologies have helped facilitate an economy where the collection of people's personal information increasingly puts them in harm's way. The number of reports received by the Federal Trade Commission regarding fraud and identity theft has skyrocketed from 224,000 complaints in 2001 to 3.6 million last year.¹⁸

These problems affect millions of Americans annually.

In 2023, the FTC received more complaints about identity theft — over 1 million complaints from consumers — than any other category.¹⁹ 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, or an authority figure requesting money or personal information. In 2023, consumers lost nearly \$2.7 billion to imposter scams.²⁰ The more personal information scammers have about a consumer's life, the more convincing these scams become. With artificial intelligence making it even easier to create convincing

In 2023, the FTC received more complaints about identity theft — over 1 million complaints from consumers — than any other category.

¹⁸ FTC, *Consumer Sentinel Network Databook 2023* (Feb. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf.

¹⁹ *Id.*

²⁰ *Id.*

deepfake images, audio, and video, data security and privacy are even more important to protect yourself from scams.

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.²¹

The best way to protect consumer data is not to collect or 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 strong data minimization rules.

Using data to profile consumers often leads to discriminatory outcomes.

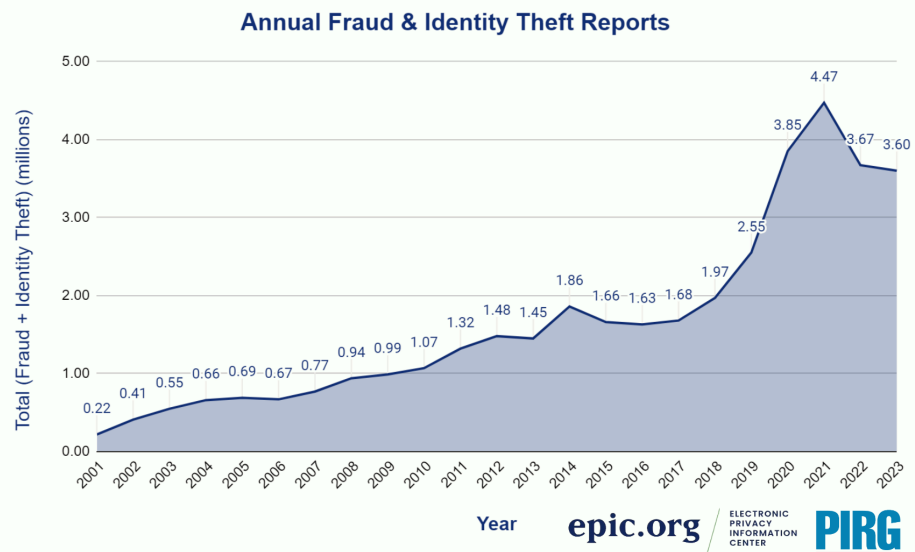
In many cases, the massive collection of data in the hands of data brokers means that consumers are sorted and scored in discriminatory ways.²² Data brokers build detailed profiles about individuals with information ranging from basic contact information to purchasing habits to sensitive information 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.” These labels — whether accurate or not — become part of that consumer’s profile and affect what products are marketed to them, what job postings they see, and what price they pay for various products and services.

²¹ 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>.

²² 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>.



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.²³ Despite never directly interacting with you, data brokers 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.

Online platforms and ad tech companies use these ever-growing profiles to shape customers' experience of the websites they visit in ways that are entirely opaque to them. These profiles are used to alter what we see, what prices we pay, and whether we can 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 ad 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.²⁴ 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.²⁵

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 prohibiting 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.²⁶ While consumers can protect

²³ 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-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

²⁴ 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.

²⁵ *Id.*

²⁶ USCDornsife, *Thinking vs. Feeling: The Psychology of Advertising* (Nov. 17, 2023), <https://appliedpsychologydegree.usc.edu/blog/thinking-vs-feeling-the-psychology-of-advertising>.

their mailboxes from junk mail and phones from spam calls, there is 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 who meet specific parameters. People searching terms like “need money help” on Google have been served ads for predatory loans with staggering interest rates of over 1,700%.²⁷ An online casino targeted ads to problem gamblers offering them free spins on its site.²⁸ 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.²⁹

Advertising can still serve businesses' objectives without relying on collecting and selling personal data that unnecessarily puts consumers in harm's way. Many companies rely instead on contextual advertising, which allows them to serve ads related to the topic a person searched on a search engine or the content on the webpage a person is viewing. For example, a company that sells running shoes would likely find its intended audience by advertising on a health and fitness podcast. 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 users' browsing history or creating 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 increases consumer interest by 32% and that 85% of consumers who saw contextual ads instead of targeted ads were more open to seeing future ads.³⁰

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 could still offer goods and services, and advertising would still be successful. 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. They oppose legislation that protects your privacy to keep these practices running. And because of their outsized influence on policy, Americans are left with weak privacy laws that do little to protect consumers. The rules we

²⁷ 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>.

²⁸ 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>.

²⁹ 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>.

³⁰ 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>.

propose in this report allow companies to continue advertising to their intended customers in a way that doesn't involve ubiquitous tracking of consumers' every movement online.

Despite these urgent harms, Congress has failed to pass federal privacy legislation.

The U.S. still lacks a comprehensive federal privacy law. Congress has considered bipartisan privacy legislation twice since 2022 yet failed to enact a privacy law either time. The American Data Privacy and Protection Act (ADPPA) was introduced in 2022 and went through extensive negotiations between members of Congress from both parties, industry, civil rights groups, and consumer protection and privacy groups.³¹ The bill set a strong data minimization standard for the collection and use of personal data, contained robust civil rights protections, and gave individuals the right to sue if their privacy rights were violated. The proposal received overwhelming bipartisan support in the House Energy & Commerce Committee, where it was favorably approved on a 53-2 vote.³² Unfortunately, Congress failed to enact ADPPA.

In 2024, another privacy bill was introduced: The American Privacy Rights Act (APRA), which contained many of the same provisions as ADPPA and aimed to build off ADPPA's momentum and consensus.³³ It was introduced by bipartisan leaders on the Senate Commerce Committee and House Energy & Commerce Committee: Sen. Maria Cantwell [D] and Rep. Cathy McMorris Rodgers [R]. However, disagreements over anti-discrimination provisions among other Members led to stalled progress on the bill, and it never received a Committee markup.

Why this is happening: Big Tech has been allowed to write its own rules

The opaque world of data harvesting and sales is becoming more visible. People are increasingly concerned about protecting their privacy. State legislators want to take action. We have the ingredients for meaningful change. How is it that we have ended up with so many laws that fail to give consumers meaningful protections?

Unfortunately for consumers, a coordinated lobbying effort on behalf of some of the biggest tech companies in the world has successfully pushed weak legislation in many states that does much more to help the corporations profiting off of mass data collection than it does to protect consumers whose data is being harvested.³⁴

³¹ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

³² *Id.*

³³ American Privacy Rights Act, H.R. 8818, 118th Cong. (2024).

³⁴ See Alfred Ng, *The Man Quietly Rewriting American Privacy Law*, Politico (Sept. 18, 2024), <https://www.politico.com/news/2024/09/17/andrew-kingman-data-privacy-lobbying-00179630>; Todd

How the tech industry's favored privacy bill became the standard across the states

The heavy involvement of tech industry lobbyists in pushing weak privacy laws at the state level began almost immediately after California passed its first-in-the-nation privacy law in 2018, which provided real protections for California residents. In response, lobbyists for industry players including Amazon, Comcast, and Microsoft began pushing Washington state to weaken its Washington Privacy Act, which was moving through the state's Legislature in 2019.³⁵ While the bill ultimately failed to pass in Washington, it quickly became the standard industry urged states considering privacy legislation to adopt.

This strategy worked. Virginia became the second state in the nation to pass a comprehensive consumer data privacy law in 2021. Virginia's legislation, which was based on the industry-influenced Washington Privacy Act, had been handed to the bill sponsor by an Amazon lobbyist, and it was almost entirely devoid of usable privacy protections for consumers. Companies could continue collecting whatever data they wanted as long they disclosed it somewhere in a privacy policy. While consumers could, in theory, request 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.

Unfortunately, Virginia became the model lobbyists have pushed many state legislators to match, particularly in red states such as Kentucky and Montana.³⁶ Kentucky Sen. Whitney Westerfield tried to counter this pressure for the state to pass a weak privacy bill by running a strong privacy bill over multiple years. Sen. Westerfield's bill passed the Senate in 2023, but the state ultimately enacted a Virginia-style bill.³⁷ In a Vermont hearing about industry lobbying on state privacy bills,

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>.

³⁵ Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, Protocol (Feb. 19, 2021), <https://web.archive.org/web/20240218235654/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/>.

³⁶ 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>.

³⁷ S.B. 15, 2023 Gen. Assemb., Reg. Sess. (Ky. 2023).

Sen. Westerfield said, “Everyone said . . . ‘follow Virginia. Virginia is the model.’ No one could explain why Virginia was the model, that was just the model they all went with.”³⁸

Along with Kentucky, five more states adopted versions of the Virginia law: Indiana, Iowa, Nebraska, Tennessee, and Utah. These states all received Fs on this scorecard.

More recently, and particularly in blue states, lobbyists have pivoted to pushing the “Connecticut model” — a bill similar to Virginia but with a couple additional consumer protections.³⁹ 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 previously — notably from his 2020 privacy bill, which included the ability for consumers to sue.⁴⁰ Connecticut, in this scorecard, receives a D.

In 2023 and 2024, the pressure and the strategy from industry remained the same: Convince as many states as possible to pass laws that look as identical to the Virginia/Connecticut “models” as possible. Using the guise of “interoperability,” lobbyists consistently seek to convince lawmakers that passing any law with stronger protections — such as data minimization requirements or a private right of action — will be detrimental to their state’s economy and to its residents.

In Oregon, for example, the State Privacy and Security Coalition — a misleadingly named industry group representing Amazon and Meta, among others⁴¹ — testified at one point that a stronger draft of the Oregon Consumer Privacy Act “deviate[d] from other state privacy laws” as to “need

³⁸ Hearing before the Vermont House Committee on Commerce and Economic Development (Apr. 26, 2024), <https://www.youtube.com/watch?v=RfvAteuwRCA> (testimony of Kentucky Senator Whitney Westerfield).

³⁹ 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.”)

⁴⁰ 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>.

⁴¹ State Privacy and Security Coalition, *About SPSC* (web page), archived on Dec. 9 2024, <https://web.archive.org/web/20241209193414/https://thespsc.org/about-us/>; Suzanne Smalley, *In Patchwork of State Privacy Legislation, Tech Lobby Sees a Single Battlefield*, The Record (Jan. 30, 2024), <https://therecord.media/state-data-privacy-legislation-technology-industry-lobbying>.

significant work.”⁴² Maryland Sen. Sara Love, who sponsored the privacy law that passed there in 2024, testified that: “State Privacy and Security [Coalition] gave us a redline of our bill. It was not, ‘Do you have specific amendments?’ It was, ‘We are redlining your bill to be Virginia or Delaware or pick your other state that follows the similar industry model.’”⁴³ In Delaware, the Computer Communications Industry Association — an industry group representing Google and Apple, among others⁴⁴ — 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.⁴⁵

Due to this lobbying pressure, of the 19 comprehensive privacy laws passed so far, the vast majority closely follow a model that was initially drafted by industry giants such as Amazon.⁴⁶

‘Big Tech has a playbook’

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 31 states that heard privacy bills in 2021 and 2022. Because of the opacity of state lobbying records, that number is likely an undercount.⁴⁷

A 2023 analysis of state tech lobbying found that in the 19 states with thorough lobbying disclosure requirements, major tech and industry lobbying groups spent \$13.4 million.⁴⁸ This figure is triple what tech lobbyists spent in these states a decade ago.⁴⁹ While hard data on the time and money spent by tech and industry lobbying efforts can be challenging to find in some states, anecdotal evidence from state lawmakers across the country abounds.

⁴² 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>.

⁴³ Hearing before the Vermont House Committee on Commerce and Economic Development (Apr. 26, 2024), <https://www.youtube.com/watch?v=RfvAteuWRCA> (testimony of Maryland Senator Sara Love).

⁴⁴ Computer Communications Industry Association, *Our Members*, archived Dec. 18, 2024 at <https://web.archive.org/web/20241218202941/https://ccianet.org/>.

⁴⁵ 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/>.

⁴⁶ 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/>.

⁴⁷ Feathers & Ng, *supra* note 34.

⁴⁸ Austin Jenkins, *Tech Lobbying Spending Surges in States*, Pluribus News (June 7, 2024), <https://pluribusnews.com/news-and-events/tech-lobbying-spending-surges-in-states/>.

⁴⁹ *Id.*

Nearly all state lawmakers who have introduced strong privacy legislation faced a torrent of industry lobbying trying to weaken or kill their bills. To bring attention to some of the most common industry tactics, Vermont Rep. Monique Priestley, who sponsored the state’s strong privacy bill, invited lawmakers from 5 other states and both sides of the aisle to testify about their experiences.

The legislators all spoke to the sheer volume of lobbyists fighting to weaken their bills. When Maine was considering privacy legislation in 2024, Rep. Maggie O’Neil — the sponsor of a strong privacy bill that failed to pass by only a handful of votes on the last day of the legislative session — recounted seeing “more lobbyists hired in the building than I have ever seen on bills before” in her 8 years in the Legislature.⁵⁰ Sen. Love testified that it was a similar story in Maryland: “I will tell you, I have not in my six years, in my second term, seen as hard a lobbying job as these folks did. They put so much money into pushing and lobbying,” Sen. Love said.⁵¹

After each state legislator testified, Rep. Priestley and the other Vermont Representatives would reflect on how similar their experience was to those their colleagues in Maine, Maryland, Oklahoma, Kentucky, and Montana described.⁵² Despite these lawmakers being from different parties in states spanning the country, the tech industry tactics they faced were nearly identical. “The biggest thing I have learned from this entire bill is that Big Tech has a playbook,” Rep. Priestley said in a Politico article about the hearing.⁵³

A key strategy Big Tech uses across states is to rely on trade groups and business organizations to openly criticize strong bills rather than testifying against bills themselves. Rep. O’Neil noticed this tactic in Maine: “Very rarely did we hear directly from a Facebook or a Google or an Amazon. There were organizations that lobbied on their behalf . . . like TechNet or State Privacy and

⁵⁰ Hearing before the Vermont House Committee on Commerce and Economic Development (Apr. 26, 2024), <https://www.youtube.com/watch?v=RfvAteuwRCA> (testimony of Maine Representative Maggie O’Neil).

⁵¹ Hearing before the Vermont House Committee on Commerce and Economic Development (Apr. 26, 2024), <https://www.youtube.com/watch?v=RfvAteuwRCA> (testimony of Maryland Senator Sara Love).

⁵² Hearing before the Vermont House Committee on Commerce and Economic Development (Apr. 26, 2024), <https://www.youtube.com/watch?v=RfvAteuwRCA> (statements of Vermont Representative Monique Priestley).

⁵³ Alfred Ng, *Vermont’s Data Privacy Law Sparks State Lawmaker Alliance Against Tech Lobbyists*, Politico (May 18, 2024), <https://www.politico.com/news/2024/05/18/vermont-data-privacy-law-tech-lobbyists-00158711>.

Security Coalition.”⁵⁴ TechNet and the State Privacy and Security Coalition are both funded in part by Meta, Google, and Amazon.⁵⁵

Local businesses denied working with Big Tech to coordinate their opposition.⁵⁶ However, Politico obtained an email from a State Privacy and Security Coalition (SPSC) lobbyist to local Vermont business groups—including the Vermont Chamber of Commerce, the Vermont Retail & Grocers Association, and the Vermont Ski Areas Association—coordinating efforts to oppose a strong privacy bill with a private right of action.⁵⁷ This SPSC lobbyist also held weekly calls with Vermont business organizations from the time the draft of the bill was introduced through the end of Vermont’s legislative session to coordinate pushback against the bill.⁵⁸

Politico found that the State Privacy and Security Coalition worked to oppose and water down strong privacy bills—or to support bills similar to the weak industry model—in at least 32 states.⁵⁹

Kentucky is one state where the bill’s sponsor said he felt there was coordination between the State Privacy and Security Coalition and the local Chamber of Commerce. Kentucky Sen. Whitney Westerfield worked to pass a strong privacy bill that included a private right of action, but he faced fierce pushback from business and industry groups. An SPSC lobbyist “worked to sink [Sen. Westerfield’s] proposal over provisions giving people the right to sue companies that violate the privacy law.”⁶⁰ Sen. Westerfield, who testified in the Vermont hearing on lobbying efforts against strong privacy bills, said, “While I was busy trying to get my bill out of the Senate, the Chamber was busy holding it back. They were working hard in the House poisoning the well.”⁶¹ This opposition from national and local groups succeeded in Kentucky; the state failed to pass Westerfield’s strong bill in favor of the industry-backed Virginia “model.” Kentucky’s law receives an F on our scorecard.

⁵⁴ Hearing before the Vermont House Committee on Commerce and Economic Development (Apr. 26, 2024), <https://www.youtube.com/watch?v=RfvAteuwRCA> (testimony of Maine Representative Maggie O’Neil).

⁵⁵ These companies are listed as members to the trade groups. Generally speaking, being a member of a trade group requires paying dues to receive benefits, including access to state lobbying on behalf of members’ interests, regular updates on legislative activity, and assistance with strategic communication. See TechNet, *Members* (web page), archived on Dec. 9, 2024, <https://web.archive.org/web/20241209193133/https://www.technet.org/our-story/members/>; TechNet, *Benefits of Membership* (web page), archived on Dec. 18, 2024, <https://web.archive.org/web/20241218205015/https://www.technet.org/our-story/members/benefits-of-membership/>. State Privacy and Security Coalition, *About SPSC* (web page), archived on Dec. 9 2024, <https://web.archive.org/web/20241209193414/https://thespsc.org/about-us/>.

⁵⁶ Ng, *supra* note 53.

⁵⁷ Ng, *supra* note 34.

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ Hearing before the Vermont House Committee on Commerce and Economic Development (Apr. 26, 2024), <https://www.youtube.com/watch?v=RfvAteuwRCA> (testimony of Kentucky Senator Whitney Westerfield).

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 harder it becomes for states to stray from those models. However, the tide is beginning to turn.

State lawmakers are increasingly championing meaningful privacy protections instead of settling for the industry model

In 2024, state legislators across the country pushing back against outsized industry influence saw the first significant signs of success.

After several years of considering privacy legislation, Maryland passed one of the strongest privacy laws in the country in 2024. The Maryland Online Data Privacy Act includes strong data minimization requirements limiting the collection of personal data, prohibits the sale of sensitive data, bans targeted advertising to children and teens, and contains limited exemptions — all provisions that industry lobbyists fight against.⁶²

Sen. Love, the bill sponsor, credits the bill's success to her fellow lawmakers' willingness to see through industry's tactics and remain dedicated to passing a strong bill with meaningful privacy protections. "The more [lobbyists] pushed, the more we said — and not just me, also other legislators said — 'Enough. We're going to pass something that matters.'"⁶³

Consumer privacy advocates hope Maryland's success in enacting a protective privacy law will incentivize other states to also pass strong laws. A few other states also made notable progress in 2024 toward enacting strong privacy protections for their residents.

Vermont and Maine both came very close to passing what would have been two of the strongest privacy laws in the country. The Vermont Legislature passed a privacy bill with meaningful data minimization requirements, strong civil rights language, and a private right of action.⁶⁴ Despite the bill garnering widespread support from lawmakers of all political parties and passing unanimously in the House, Gov. Phil Scott vetoed the legislation.⁶⁵ The House voted overwhelmingly to override the governor's veto, but the Senate was a few votes shy of successfully overriding in its chamber.⁶⁶

⁶² Md. Code Ann. Com. Law § 14-4601.

⁶³ Hearing before the Vermont House Committee on Commerce and Economic Development (Apr. 26, 2024), <https://www.youtube.com/watch?v=RfvAteuwRCA> (testimony of Maryland Senator Sara Love).

⁶⁴ H. 121, 2024 Gen. Assemb. (Vt. 2024).

⁶⁵ Veto letter from Vermont Governor Phil Scott, Office of the Governor of the State of Vermont (June 13, 2024), <https://governor.vermont.gov/sites/scott/files/documents/H.121%20-%20Veto%20Letter.pdf>.

⁶⁶ EPIC, *Vermont Senate Fails to Override Vermont Data Privacy Act Veto* (June 19, 2024), <https://epic.org/vermont-senate-sustains-governors-veto-of-vermont-privacy-act/>.

While it is unfortunate that Vermonters are still without privacy protections, bill sponsor Rep. Monique Priestley has said she is committed to running a strong data privacy bill again this year.⁶⁷ Given her experience facing massive industry lobbying on her bill in 2024 and her understanding of what has happened in other states, Rep. Priestley said she anticipates Big Tech to work with a fellow lawmaker to file a competing, Connecticut/Virginia-style bill. However, she is not deterred by this and said she “is going to come with an even stronger, tightened up House version” of the strong privacy bill that passed the Legislature this session.⁶⁸

Maine also came within a few votes of passing a strong privacy bill this year. Rep. Maggie O’Neil introduced several strong privacy bills, including a comprehensive privacy bill that contained data minimization requirements and a private right of action.⁶⁹ Another Maine legislator pushed a weak bill modeled off of Connecticut.⁷⁰ These competing privacy bills went through more than 30 hours of working sessions during which Maine legislators carefully compared the two bills’ differing approaches to key provisions like data minimization, protections for minors, and exemptions. Ultimately, Maine’s Judiciary Committee advanced an amended version of Rep. O’Neil’s bill and not the industry-modeled bill—though the months of negotiations did result in removal of the private right of action from the bill.⁷¹ The House of Representatives passed Rep. O’Neil’s bill, but the proposed legislation just short of passing the Senate, leaving Mainers without privacy protections for another year.⁷² Rep. O’Neil has reached Maine’s term limit for serving in the Legislature. Still, she said she hopes other lawmakers on the Judiciary Committee who have invested so many hours into data privacy will continue her work in the upcoming legislative session.⁷³

Massachusetts and Illinois introduced strong privacy bills in 2024 modeled off the bipartisan federal proposal from 2022, the American Data Privacy Protection Act (ADPPA). The

⁶⁷ Scott M Graves, *Innova802: The Battle for Data Privacy Rights in Vermont*, Are We Here Yet Podcast (July 22, 2024), <https://open.spotify.com/episode/12fkh7CDyaivBniVJQ4uqX?si=VEDDE--yTWuZJF0m0A9rtA&nd=1&dlsi=65454f284e064b92>.

⁶⁸ *Id.*

⁶⁹ L.D. 1977, 131st Leg., 2d Reg. Sess. (Me. 2024).

⁷⁰ L.D. 1973, 131st Leg., 2d Reg. Sess. (Me. 2024).

⁷¹ Emma Davis, *Maine Lawmakers Advance What Could Be One of Nation’s Toughest Data Privacy Laws*, *Maine Morning Star* (Mar. 28, 2024), <https://mainemorningstar.com/2024/03/28/maine-lawmakers-advance-what-could-be-one-of-nations-toughest-data-privacy-laws/>.

⁷² Keely Quinlan, *Maine Fails to Pass Ambitious Consumer Data Privacy Act*, *StateScoop* (Apr. 17, 2024), <https://statescoop.com/maine-consumer-data-privacy-bill-fails-2024/>.

⁷³ Emma Davis, *Legislature Rejects Paths to a Comprehensive Data Privacy Law in Maine*, *Maine Morning Star* (Apr. 18, 2024), <https://mainemorningstar.com/2024/04/18/legislature-rejects-paths-to-a-comprehensive-data-privacy-law-in-maine/>.

Massachusetts Joint Committee on Advanced Information Technology, the Internet, and Cybersecurity favorably reported the bill.⁷⁴

It is critical that lawmakers capitalize on this momentum and continue pushing for meaningful privacy protections. States can pass strong privacy laws—Maryland’s enactment of the Maryland Online Data Privacy Act and the Vermont Legislature’s overwhelming support for the Vermont Data Privacy Act prove that. More states can join the effort to protect privacy for everyone by introducing legislation consistent with the recommendations in this report.

The solution: What a strong privacy law looks like

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

Features of strong state-level regulations

Existing state privacy laws 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.

⁷⁴ Bill S.2770, 193d Gen. Ct. (Mass. 2024).

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 of providing the goods or services that they requested.

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

Companies should not have a limitless ability to decide how much personal data to collect. Unfortunately, this is what all state laws — other than California’s and Maryland’s — allow. By following the Virginia/Connecticut “model,” all other state laws only limit collection to what is reasonably necessary for “the purposes for which such data is processed, as disclosed to the consumer,” meaning businesses can collect data for whatever purposes they want, as long as they state that purpose in their privacy policies. 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 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.
- The sale of sensitive data should be prohibited.
- 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.

So far, no state has enacted the full data minimization outlined above. California and Maryland both enacted laws with some data minimization requirements, representing significant improvements over the Virginia/Connecticut-style laws. However, there is more that states can do to protect the privacy of their residents.

Data minimization is essential for both consumers and businesses. Data minimization principles give consumers confidence in using technology, knowing there are rules 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 businesses are collecting less personal data about consumers and promptly deleting data they no longer need. Ultimately, this means businesses have less data overall, making it less likely that consumer data will be exposed in a data breach.

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.

ENFORCEMENT							
State	AG rulemaking	AG enforcement authority	Right to cure*	Private right of action	Injunctive relief	Statutory damages	Privacy Agency
CA	✓	✓	DISC	✓	✓	✓	✓
CO	✓	✓	SUN	✗	✗	✗	✗
CT	✗	✓	SUN	✗	✗	✗	✗
DE	✗	✓	SUN	✗	✗	✗	✗
IA	✗	✓	MAND	✗	✗	✗	✗
IN	✗	✓	MAND	✗	✗	✗	✗
KY	✗	✓	MAND	✗	✗	✗	✗
MD	✗	✓	DISC	✗	✗	✗	✗
MN	✗	✓	SUN	✗	✗	✗	✗
MT	✗	✓	SUN	✗	✗	✗	✗
NE	✗	✓	MAND	✗	✗	✗	✗
NH	✓	✓	SUN	✗	✗	✗	✗
NJ	✓	✓	SUN	✗	✗	✗	✗
OR	✗	✓	SUN	✗	✗	✗	✗
RI	✗	✓	NONE	✗	✗	✗	✗
TN	✗	✓	MAND	✗	✗	✗	✗
TX	✗	✓	MAND	✗	✗	✗	✗
UT	✗	✓	MAND	✗	✗	✗	✗
VA	✗	✓	MAND	✗	✗	✗	✗

DISC = Discretionary SUN = Sunset MAND = Mandatory

However, while government enforcement is essential, the scope of data collection online is too vast for one entity to regulate, particularly state Attorneys General, who have broad mandates and limited resources. Individuals who use these online services are in the best position to identify privacy issues and take action to protect their privacy. A private right of action preserves the state's resources, and the threat of statutory damages is a strong motivator to incentivize compliance with 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 controllers have strong financial incentives to comply with state privacy laws. We have seen evidence of this in Illinois,⁷⁵ 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.⁷⁶

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 guiding 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.⁷⁷ These issues make existing laws insufficient to protect all people from digital discrimination. 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.”

This year, Maryland and Minnesota passed privacy laws that included a stronger civil rights provision than any existing state’s privacy law by adopting a version of the above language. However, the language in these two laws only prohibits discrimination that is already unlawful under current state laws. Ideally, states should adopt the above language without limiting protections to already unlawful discrimination to ensure that data can’t be used to discriminate.

⁷⁵ Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), <https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf>.

⁷⁶ 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>.

⁷⁷ 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>.

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 similar risk assessments, which can help with meaningful oversight, if done correctly.

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

These assessments should include documentation of what personal data is collected, why that personal data is 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 the controller rejected those alternatives.

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.

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 become internal box-checking exercises.⁷⁸

⁷⁸ See generally Ari Ezra Waldman, *Industry Unbound* (2021) (demonstrating that many privacy impact assessments conducted under GDPR have become little more than checkbox forms).

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 are an important component of any comprehensive privacy bill.

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

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

1. Require companies to honor universal opt-out signals.

Many states have included this requirement in their privacy laws.

2. 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").

3. Consumers should know who has their data.

Oregon, Delaware, Maryland and Minnesota provide the right to obtain information about third parties to whom a company disclosed your personal data or the personal data of consumers generally.

4. 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 Consumer Reports have found that it helps make consumers' individual rights more meaningful.⁷⁹

⁷⁹ Kaveh Waddell, *How 'Authorized Agents' Plan to Make It Easier to Delete Your Online Data*, Consumer Reports (Mar. 21, 2022),

Banning manipulative design and unfair marketing

UNFAIR BUSINESS PRACTICES			
State	Civil Rights Protection	Loyalty program data limits	Prohibits dark patterns
CA	✗	✓	✓
CO	✗	✗	✓
CT	✗	✗	✓
DE	✗	✗	✓
IA	✗	✗	✗
IN	✗	✗	✗
KY	✗	✗	✗
MD	✓	✓	✓
MN	✓	✗	✓
MT	✗	✗	✓
NE	✗	✗	✓
NH	✗	✗	✓
NJ	✗	✗	✓
OR	✗	✗	✓
RI	✗	✗	✓
TN	✗	✗	✗
TX	✗	✗	✓
UT	✗	✗	✗
VA	✗	✗	✗

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.

Second, states should prohibit discrimination against consumers who exercise their privacy rights. Businesses should not be permitted to charge consumers higher prices for goods if they have opted out of targeted advertising.

Third, “dark patterns,” or manipulative design meant to subvert consumer choice, should be prohibited in both the definition of consent and 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.

<https://www.consumerreports.org/electronics/privacy/authorized-agents-plan-to-make-it-easier-to-delete-your-data-a8655835448/>.

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:

STRONG KEY DEFINITIONS								
State	Personal/covered data	Pseudonymous exemption	Biometric data	Covered entity/controller	Narrow carveouts	Sell/share	Profiling	Targeted ads
CA	✓	✓	✗	✓	✓	✓	✓	✓
CO	✓	✓	✓	✓	✓	✗	✓	✓
CT	✗	✓	✗	✓	✗	✗	✓	✓
DE	✗	✓	✗	✓	✓	✗	✓	✓
IA	✗	✗	✗	✓	✗	✗	✗	✓
IN	✗	✗	✗	✓	✗	✗	✓	✓
KY	✗	✓	✗	✓	✗	✗	✓	✓
MD	✓	✓	✓	✓	✓	✗	✓	✓
MN	✗	✓	✗	✓	✓	✗	✓	✓
MT	✗	✓	✗	✓	✗	✗	✓	✓
NE	✓	✗	✗	✓	✗	✗	✓	✓
NH	✗	✓	✗	✓	✗	✗	✓	✓
NJ	✗	✓	✗	✓	✓	✗	✓	✓
OR	✓	✓	✓	✓	✓	✗	✓	✓
RI	✗	✗	✗	✓	✗	✗	✓	✓
TN	✗	✗	✗	✗	✗	✗	✓	✓
TX	✗	✗	✓	✗	✗	✗	✓	✓
UT	✗	✓	✓	✗	✗	✗	✗	✓
VA	✗	✗	✗	✓	✗	✗	✓	✓

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 collect mass amounts of 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 as a whole. Two of the most common entity-level exemptions in state laws are for entities covered by the federal Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA). GLBA is outdated privacy legislation that primarily requires financial institutions to mail privacy notices that offer an opt out of disclosure to third parties. GLBA does not provide even basic access or deletion rights. Similarly, HIPAA protects only health data in the hands of a healthcare provider, plan, or clearinghouse—importantly, not information in the hands of health apps or websites. It is inappropriate to exempt entire entities from coverage of a comprehensive privacy law simply because a federal law with limited privacy protections covers some of the data they collect. Instead, if states do want to provide exemptions, they should include only data-level exemptions for the specific information already regulated by another federal privacy law.

Other common exemptions are nonprofits and institutions of higher education, which privacy laws should also cover. These entities often handle large amounts of personal data, so they should have to comply with privacy regulations.

The Connecticut Attorney General has also flagged these overly broad exemptions as a flaw with Connecticut’s privacy law that the Legislature should fix. In a report from early 2024, the Connecticut AG recommended that the Legislature “scale back the entity-level exemptions in CTDPA” because they “put Connecticut residents at a disadvantage.”⁸⁰ Specifically, the AG’s report recommends that the Legislature narrow the exemptions for nonprofits and entities regulated by HIPAA and GLBA.⁸¹ The federal Consumer Financial Protection Bureau also released a report in November 2024 warning that state privacy laws that contain entity-level exemptions for GLBA leave a significant amount of consumers’ financial data unprotected.⁸²

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 disclosing personal data to facilitate targeted advertising, whether or not for monetary or other valuable consideration. Many

⁸⁰ Connecticut Office of the Attorney General, *Report to the General Assembly’s General Law Committee Pursuant to Public Act 22-15, “An Act Concerning Personal Data Privacy and Online Monitoring” Referred to as the Connecticut Data Privacy Act (“CTDPA”)*, (Feb. 1, 2024), https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf?rev=8fbba0ba237a42748d3ad6544fd8228c&hash=41BCE2F7485413487EE5F534E6AC6C60.

⁸¹ *Id.*

⁸² Press Release, *CFPB Report Details Carveouts for Financial Institutions in State Data Privacy Laws*, Consumer Financial Protection Bureau (Nov. 12, 2024), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-report-details-carveouts-for-financial-institution-s-in-state-data-privacy-laws/>.

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 "sold" in these instances, these uses fall outside of many states' definitions. Closing this loophole 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,⁸³ 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. This overly narrow definition of biometric data has also been an area of concern for the Connecticut Attorney General's Office, which released a report in February recommending several amendments to the Connecticut Data Privacy Act.⁸⁴ One of the Attorney General's suggested amendments was for the Legislature to revise the definition of biometric data to align with the language we suggested above, which other states have also adopted.

⁸³ Irish Council for Civil Liberties, *supra* note 16; Sara Morrison, *Meta Is Getting Data About You from Some Surprising Places*, Vox, (June 17, 2022), <https://www.vox.com/recode/23172691/meta-tracking-privacy-hospitals>.

⁸⁴ Connecticut Office of the Attorney General, *supra* note 80.

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

We evaluated each of the 19 state comprehensive consumer privacy laws enacted as of December 2024.

We graded the state laws based on the above-mentioned provisions — elements that would be found in a privacy law that provides meaningful consumer protections. The most important aspects of a strong privacy law — data minimization requirements, vigorous 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 19 laws, nearly half received a failing grade. None received an A.

Advancing “B” states

California

California Consumer Privacy Act

Date law took effect: January 1, 2020

Score: 69/100



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, strengthening the 2018 law. Today, California's privacy law is one of the strongest in the nation, though it lacks many critical consumer protections. In 2023, California passed the DELETE Act,⁸⁵ allowing California residents to make one deletion request that all data brokers in the state must comply with. While the CCPA extends the right to delete only to personal information provided by the consumer, the DELETE Act 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
- Limits businesses' collection, use, and retention of personal data to purposes that are in line with consumers' expectations or the consumer has affirmatively consented to
- Prohibition on 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
- Default limits on cross-site browser tracking, rather than an opt-out
- 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.

⁸⁵ Cal. Civ. Code § 1798.99.86 (West 2023).

Maryland

Maryland Online Data Privacy Act

Date law will take effect: October 1, 2025

Score: 51/100

B-

Maryland enacted one of the strongest state privacy laws in the country this year when it enacted the Maryland Online Data Privacy Act. The base text of the Maryland law is similar to the Connecticut Data Privacy Act, but was strengthened by the addition of strong data minimization provisions that require companies to better align their data collection policies with consumers' expectations and a ban on the sale of sensitive data. Maryland's law provides a model of how Connecticut-style laws can be strengthened to more meaningfully protect privacy.

Privacy-protective provisions:

- Data minimization requirement that controllers limit collection of personal data to only what is reasonably necessary and proportionate to provide or maintain a product or service requested by the consumer
- Heightened protections for sensitive data
- Ban on the sale of sensitive data
- Ban on targeted advertising to minors under 18
- Prohibition on controllers requiring consumers to consent to the sale of their personal data as a condition of participating in loyalty programs
- Additional 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
- No exemption for pseudonymous data

Missing provisions:

- No private right of action
- No Attorney General rulemaking authority

Possible amendments:

- Expand data minimization requirements to include controllers' use of such data.
- Change carveout for GLBA from all financial institutions covered by the law to only the data that is regulated by the law.
- Require controllers to make impact assessments (or a summary) available to the public.
- Expand authorized agent provisions to allow consumers to authorize agents to exercise all consumer rights instead of only opt-out rights.

The middling “C” states

Colorado

Colorado Privacy Act

Date law took effect: July 1, 2023

Score: 42/100



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 an universal opt-out mechanism. In July 2024, Colorado residents gained the ability to download and use the Global Privacy Control (GPC) tool to automatically broadcast to websites that they don't want their data collected. (You can download GPC [here](#), and see CoPIRG's consumer guide [here](#).)

Privacy-protective provisions:

- Attorney General has rulemaking authority
- Requirement that controllers 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 controllers 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



New Jersey Data Privacy Law

Date law took effect: January 16, 2025

Score: 37/100

The New Jersey Legislature passed the New Jersey Data Privacy Law in January 2024. While the law still largely follows the Connecticut “model,” New Jersey made two significant improvements. First, New Jersey granted its Attorney General rulemaking authority to carry out its law, allowing the state to keep pace with rapidly evolving technological changes and ensure that the Attorney General can implement the law effectively. Second, New Jersey closed a large loophole by limiting the HIPAA exemption to carve out only the data covered by HIPAA, rather than all entities regulated by the federal law.

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 controllers 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.

Minnesota

Minnesota Consumer Data Privacy Act

Date law will take effect: July 31, 2025

Score: 32/100



After working on data privacy for multiple years, the Minnesota Legislature passed the Minnesota Consumer Data Privacy Act in 2024. This law largely still follows the Connecticut “model,” but Minnesota made several key improvements, including limiting exemptions, adding a series of consumer rights specific to profiling, and including a data minimization provision for data retention.

Privacy-protective provisions:

- Limited carveouts only for data regulated by other privacy laws rather than broad, entity-level exemptions
- Addition of 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
- Includes a series of new rights for consumers if a controller uses their personal data in a profiling decision, including the rights to question the results of a profiling decision, be informed of a reason for a profiling decision, review personal data used in profiling, correct any inaccurate personal data used in profiling and have the decision reevaluated, and, if feasible, be informed of what actions they could have taken or could take in the future to secure a different decision
- Requirement that controllers honor global opt-out signals
- Prohibition on controllers retaining personal data for longer than reasonably necessary for the purpose the data was collected or processed

Missing provisions:

- No private right of action
- No Attorney General rulemaking authority
- No data minimization rules limiting the collection or use of personal data

Possible amendments:

- Strengthen definitions of sell/share and biometric data.
- Require controllers to make impact assessments (or a summary) available to the public.
- Expand authorized agent provisions to allow consumers to authorize agents to exercise all consumer and opt-out rights instead of only opt-out rights for targeted advertising and personal data sales.

Oregon

Oregon Consumer Privacy Act

Date law took effect: July 1, 2024

Score: 31/100



Passed in June 2023, the Oregon Consumer Privacy Act resulted from a working group led by the Oregon Attorney General's office. Despite this, it still followed the Connecticut model, though Oregon added some important protections – including minimizing the number of entities exempted 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”
- Addition of 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 controllers to make impact assessments (or a summary) available to the public.

Delaware

Delaware Personal Data Privacy Act

Date law took 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 the 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.⁸⁶

Privacy-protective provisions:

- Ban on targeted advertising to minors under 18 years old
- Broad definition of sensitive data that includes "status as pregnant" and "status as transgender or nonbinary"
- Additional consumer right to obtain a list of the categories of third parties with whom the controller has shared the consumer's 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 regulated by the law.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require controllers to make impact assessments (or a summary) available to the public.

⁸⁶ 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 22/100



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

A year after its passage, the Connecticut Legislature passed amendments to the CTDPA to add heightened protections for kids and teens online and a category of sensitive data for “consumer health data.”

Privacy-protective provisions:

- Requirement that controllers honor global opt-out signals (though the 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 CTDPA.)

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 controllers to make impact assessments (or a summary) available to the public.

New Hampshire



New Hampshire Privacy Law

Date law took effect: January 1, 2025

Score: 22/100

The New Hampshire Legislature passed the New Hampshire Privacy Law, modeled mainly off of Connecticut's law, in January 2024. New Hampshire made one notable improvement on the Connecticut "model" by granting limited rulemaking authority to its Attorney General.

Privacy-protective provisions:

- Limited Attorney General rulemaking authority

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 controllers 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 took 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 the industry to comply with and that it would be better to introduce something closer to the Virginia model. According to Politico, he strengthened his bill after he heard the same lobbyist testify in Maryland — a blue state — that industry would be happy with a Connecticut model.

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.”⁸⁷

Privacy-protective provisions:

- Requirement that controllers 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 controllers to make impact assessments (or a summary) available to the public.

⁸⁷ Ng, *supra* note 36; Edgerton, *supra* note 36.

The failing “F” states

Below are the nine states that received an F: Rhode Island, Texas, Kentucky, Nebraska, 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 a business-friendly Virginia State Senator and handed him ready-to-go legislation that would allow Big Tech’s business model to continue uninterrupted.⁸⁸ That bill sailed from introduction to passage in about six weeks 2021 and quickly became the model pushed by the tech industry across the country.

In 2022, Utah took the Virginia model and made it even less protective for consumers, changing the law so that it only covered businesses making more than \$25 million, leaving much of Utahns’ personal data unprotected.

Iowa, Indiana, and Tennessee all passed versions of this “Virginia model” in 2023; Texas passed a law that—while not quite the “Virginia model” because it does require businesses to honor universal opt-out signals—still receives an F on our scorecard. Kentucky, Nebraska, and Rhode Island followed suit in the spring of 2024, all passing laws that earn Fs.

These laws’ dismal — and strikingly similar — scores reflect their 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.



Rhode Island

Rhode Island Data Transparency and Privacy Protection Act

Date law will take effect: January 1, 2026

Score: 18/100

Indiana

Indiana Consumer Data Protection Act

Date law will take effect: January 1, 2026

Score: 11/100

Texas

Texas Data Privacy and Security Act

Date law took effect: July 1, 2024

Score: 15/100

Tennessee

Tennessee Information Protection Act

Date law will take effect: July 1, 2025

Score: 6/100

⁸⁸ Datin, Kirkham & Kalra, *supra* note 46.

Kentucky

Kentucky Consumer Data Protection Act
Date law will take effect: January 1, 2026
Score: 14/100

Utah

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

Nebraska

Nebraska Data Privacy Act
Date law took effect: January 1, 2025
Score: 14/100

Iowa

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

Virginia

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

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 requiring businesses to honor universal opt-out signals, consumers in most of these states must play whack-a-mole with companies, telling businesses one by one not to sell their data or target them with ads.⁸⁹

Without a private right of action, consumers cannot protect the minimal privacy rights these laws provide.

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

⁸⁹ The Texas Data Privacy and Security Act is the only one of the states receiving an F on our scorecard to require businesses to honor universal opt-out signals. Despite including this requirement, the law still receives an F because it contains numerous loopholes and carveouts for entire industries and lacks many important consumer protections that should be in a consumer privacy law.

Moving forward: It's not too late to set a stronger standard

Providing consumers across the country with meaningful privacy protections is essential and long overdue.

This year, several states made clear that they are willing to go further than industry-favored models by building off existing state laws while incorporating stronger protections. In enacting the Maryland Online Data Privacy Act this year, Maryland built on Delaware's law, adding strong data minimization protections, a ban on the sale of sensitive data, and heightened protections for kids and teens. Vermont, Maine, Massachusetts, and Illinois also all made significant progress toward passing strong privacy laws with similar provisions.

EPIC and Consumer Reports recently released the State Data Privacy Act, This proposed compromise model bill that uses the industry-favored Connecticut Data Privacy Act as its base text but suggests strengthening redlines to accomplish the goals outlined in this report. The goal of the State Data Privacy Act was to:

- Limit ubiquitous online tracking;
- Encourage more privacy-protective methods of online advertising;
- Protect the most sensitive data, including data about kids and teens;
- Use language from existing state laws; and
- Allow for meaningful enforcement of the law to ensure compliance.

The State Data Privacy Act borrows existing language from strong state laws and federal bills wherever possible. While this draft does not represent the ideal privacy bill for any of the signatory organizations, it is a compromise that would meaningfully protect consumers. U.S. PIRG has endorsed the bill. Find more information about the State Data Privacy Act at: <https://epic.org/the-state-data-privacy-act-a-proposed-model-state-privacy-bill/>.

We recommended specific amendments for several states throughout this report, and all states can strengthen their existing laws (or pass strong new laws) by incorporating the criteria we laid out in our scorecard or redlines from the State Data Privacy Act. While some of these suggestions require major changes, several possible amendments are minor tweaks that legislators could easily integrate into existing laws.

States can also take a sector-by-sector approach to pass essential protections. While Washington state has struggled to pass a comprehensive law, in 2023, it passed the My Health, My Data Act,⁹⁰ which contains strong protections for consumer health data and gives Washingtonians a private right of action that allows them to enforce their rights.

⁹⁰ Wash. Rev. Code Ann. § 19.373.005 (West, Westlaw Edge through 2023 Reg. and First Special Sessions).

This year showed that states are starting to move in the right direction, but there's more work to do. The State Data Privacy Act lays out a framework that states can use to meaningfully protect their residents from unchecked mass data collection and abuse. States that have passed inadequate laws can always amend them. All states still have the ability to better protect their residents' privacy.

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 Data⁹¹ or Illinois’s Biometric Information Privacy Act⁹² were not included in this report because they cover only a narrow slice of consumer data. While sectoral privacy laws like these protect some types of information, this report focuses on state laws that aim to provide 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, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, 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 businesses with more than \$1 billion in revenue.⁹³

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. Even laws that meet the above criteria are meaningless without funding to enforce the law. 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

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

The New Jersey Attorney General has not yet issued regulations under the New Jersey Data Privacy Law. Thus, New Jersey’s score was based only on the text of its statute.

⁹¹ Wash. Rev. Code Ann. § 19.373.005 (West, Westlaw Edge through 2023 Reg. and First Special Sessions).

⁹² 740 ILCS 14/1 (West 2008).

⁹³ § 501.701 Fla. Stat. (2023).

New Hampshire granted minimal rulemaking authority to the Secretary of State. Based on this, New Hampshire received partial points in the rulemaking category.

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 could not review 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 to facilitate targeted advertising, whether or not for monetary or other valuable consideration. (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)

Appendix C: State grading tables

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

ENFORCEMENT							
State	AG rulemaking	AG enforcement authority	Right to cure*	Private right of action	Injunctive relief	Statutory damages	Privacy Agency
CA	✓	✓	DISC	✓	✓	✓	✓
CO	✓	✓	SUN	✗	✗	✗	✗
CT	✗	✓	SUN	✗	✗	✗	✗
DE	✗	✓	SUN	✗	✗	✗	✗
IA	✗	✓	MAND	✗	✗	✗	✗
IN	✗	✓	MAND	✗	✗	✗	✗
KY	✗	✓	MAND	✗	✗	✗	✗
MD	✗	✓	DISC	✗	✗	✗	✗
MN	✗	✓	SUN	✗	✗	✗	✗
MT	✗	✓	SUN	✗	✗	✗	✗
NE	✗	✓	MAND	✗	✗	✗	✗
NH	✓	✓	SUN	✗	✗	✗	✗
NJ	✓	✓	SUN	✗	✗	✗	✗
OR	✗	✓	SUN	✗	✗	✗	✗
RI	✗	✓	NONE	✗	✗	✗	✗
TN	✗	✓	MAND	✗	✗	✗	✗
TX	✗	✓	MAND	✗	✗	✗	✗
UT	✗	✓	MAND	✗	✗	✗	✗
VA	✗	✓	MAND	✗	✗	✗	✗

DISC = Discretionary


























































SUN = Sunset

MAND = Mandatory

TRANSPARENCY AND DATA SECURITY

State	Data security requirement	Privacy policy standards	Notice of policy changes	Accessible privacy policies	Impact assessments	Reasonable time	Regularly reviewed	Publicly available
CA	✓	✓	✗	✓	✓	✗	✓	✓
CO	✓	✓	✓	✓	✓	✓	✓	✗
CT	✓	✓	✗	✓	✓	✗	✗	✗
DE	✓	✓	✗	✓	✓	✓	✓	✗
IA	✓	✓	✗	✓	✗	✗	✗	✗
IN	✓	✓	✗	✓	✓	✗	✗	✗
KY	✓	✓	✗	✓	✓	✗	✗	✗
MD	✓	✓	✗	✓	✓	✓	✓	✗
MN	✓	✓	✓	✓	✓	✗	✗	✗
MT	✓	✓	✗	✓	✓	✗	✗	✗
NE	✓	✓	✗	✓	✓	✗	✗	✗
NH	✓	✓	✗	✓	✓	✗	✗	✗
NJ	✓	✓	✓	✓	✓	✓	✗	✗
OR	✓	✓	✗	✓	✓	✓	✗	✗
RI	✓	✓	✗	✗	✓	✗	✗	✗
TN	✓	✓	✗	✓	✓	✗	✗	✗
TX	✓	✓	✗	✓	✓	✗	✗	✗
UT	✓	✓	✗	✓	✗	✗	✗	✗
VA	✓	✓	✗	✓	✓	✗	✗	✗

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

UNFAIR BUSINESS PRACTICES			
State	Civil Rights Protection	Loyalty program data limits	Prohibits dark patterns
CA			
CO			
CT			
DE			
IA			
IN			
KY			
MD			
MN			
MT			
NE			
NH			
NJ			
OR			
RI			
TN			
TX			
UT			
VA			

STRONG KEY DEFINITIONS

State	Personal/ covered data	No pseudonym -ous exemption	Biometric data	Covered entity/ controller	Narrow carveouts	Sell/share	Profiling	Targeted advertising
CA	✓	✓	✗	✓	✓	✓	✓	✓
CO	✓	✓	✓	✓	✓	✗	✓	✓
CT	✗	✓	✗	✓	✗	✗	✓	✓
DE	✗	✓	✗	✓	✓	✗	✓	✓
IA	✗	✗	✗	✓	✗	✗	✗	✓
IN	✗	✗	✗	✓	✗	✗	✓	✓
KY	✗	✓	✗	✓	✗	✗	✓	✓
MD	✓	✓	✓	✓	✓	✗	✓	✓
MN	✗	✓	✗	✓	✓	✗	✓	✓
MT	✗	✓	✗	✓	✗	✗	✓	✓
NE	✓	✗	✗	✓	✗	✗	✓	✓
NH	✗	✓	✗	✓	✗	✗	✓	✓
NJ	✗	✓	✗	✓	✓	✗	✓	✓
OR	✓	✓	✓	✓	✓	✗	✓	✓
RI	✗	✗	✗	✓	✗	✗	✓	✓
TN	✗	✗	✗	✗	✗	✗	✓	✓
TX	✗	✗	✓	✗	✗	✗	✓	✓
UT	✗	✓	✓	✗	✗	✗	✗	✓
VA	✗	✗	✗	✓	✗	✗	✓	✓