

The US Consumer Privacy Law Landscape



Jordan Francis, Senior Policy Counsel for U.S. Legislation

About FPF

The Future of Privacy Forum (FPF) is a **global** non-profit, non-partisan organization based in Washington, DC that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data uses, identify the risks, and develop appropriate protections.

FPF Global Offices in DC, Singapore, Brussels, & Tel Aviv, plus policy staff in India & Kenya.

FPF Members & Teams

200+

Companies

20+

Civil Society

45+

Academics

50+

Staff & Fellows

FPF Workstreams

- U.S. Legislation & Regulation
- Youth Privacy & Online Safety
- Ad Practices
- Biometrics
- Health & Wellness
- Mobility & Location
- FPF Center for Artificial Intelligence
- Global Data Protection
 - Europe
 - Asia-Pacific
 - Africa
 - Americas

Personal Data and AI in Healthcare

The Health Data Ecosystem is Diverse

- Patients interact with medical professionals in clinics and traditional health care providers
- Wearables like smart watches collect body-based and biometric data
- Apps facilitate drug delivery or telehealth
- Retail purchases create inferences about our health conditions, diagnoses, treatments
- Browsing health-related content online contributes to targeted advertising profiles



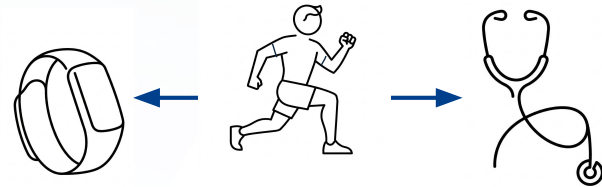
Personal Data and AI in Healthcare

Privacy in the Health Ecosystem

- Health records are protected by HIPAA and state laws
- State privacy laws regulate data revealing medical conditions or diagnoses as **sensitive data**, requiring consent
- Genetic testing laws give individuals' controls over their biological samples and genetic data

Artificial Intelligence

- Generative AI in Healthcare and AI Transcription Tools
- Automated Decisionmaking
 - Claims denials
- Health data for AI training



US Consumer Privacy Laws

- **Fragmented Federal Landscape**
- **State Comprehensive Privacy Laws**
 - 23* state comprehensive privacy laws
- **Trends**
 - Broadening Applicability
 - Expanding Scope of Sensitive Data
 - Data Minimization
 - Heightened Protections for Kids & Teens, Biometrics, Location
 - New and Expanded Consumer Rights
- **Sectoral Privacy Laws**
 - Biometrics
 - Data Brokers
 - Consumer Health
 - Genetic Testing
 - Insurance

The Federal Privacy Landscape

- **Global Outlier**

- 144 countries have a national data privacy (data protection) law, but not the U.S.

- **Sectoral Approach**

- **HIPAA:** Regulates the collection and use of **protected health information (PHI)** by **covered entities** (health plans, health care clearinghouses, and some health care providers) and **business associates** (persons who access PHI to perform certain services on behalf a covered entity)
- **COPPA:** Regulates the collection of personal information of children (under 13) by operators of websites
- **GLBA:** Regulates the collection and use of nonpublic personal information by financial institutions. Opt-out regime.

U.S. Federal Privacy Landscape

- **Sectoral Approach**

- **FCRA:** Regulates the creation and use of **consumer reports**—information communicated by a consumer reporting agency “bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living” to establish a consumer’s eligibility for purposes such as credit, insurance, or employment.
- **FTC Act, Section 5:** FTC empowered to police **unfair or deceptive acts** or practices in or affecting commerce—practices that cause or are likely to cause substantial injury to consumers which are not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.
- Other relevant laws include ECPA, VPPA, PADFAA, and more

State Activity in 2026: AI, Privacy & Youth Online Safety

4,400+

BILLS REVIEWED BY FPF

1,400+

BILLS TRACKED BY FPF

50+

BILLS ENACTED

Age-Appropriate Design Codes

Automated Decisionmaking

Biometric Identification

Chatbots & AI Companions

Comprehensive Privacy

Consumer Health

Data-Driven Pricing

Data Brokers

Employee Monitoring

Frontier Models

Generative AI & Provenance Data

Genetic Testing

Location

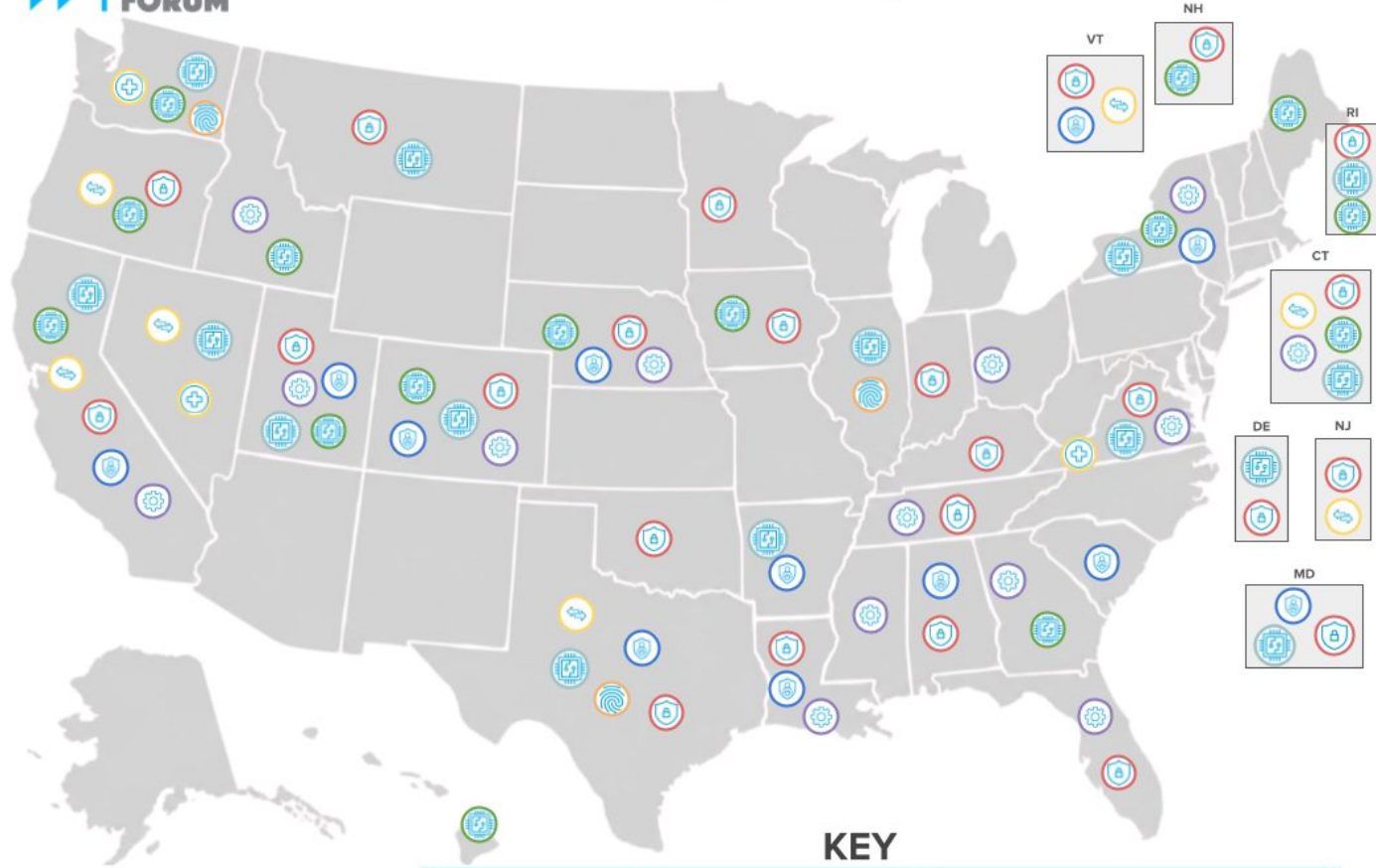
Regulatory Sandboxes

Social Media Safety

The State Privacy Landscape

- **Comprehensive Privacy Laws**
 - 23* state comprehensive privacy laws
 - Understanding the Washington Privacy Act (WPA) Framework
- **Trends**
 - Broadening Applicability
 - Expanding Scope of Sensitive Data
 - Data Minimization
 - Heightened Protections for Kids & Teens, Biometrics, Location
 - New and Expanded Consumer Rights
- **Sectoral Privacy Laws**
 - Biometrics
 - Data Brokers
 - Consumer Health
 - Genetic Testing
 - Insurance

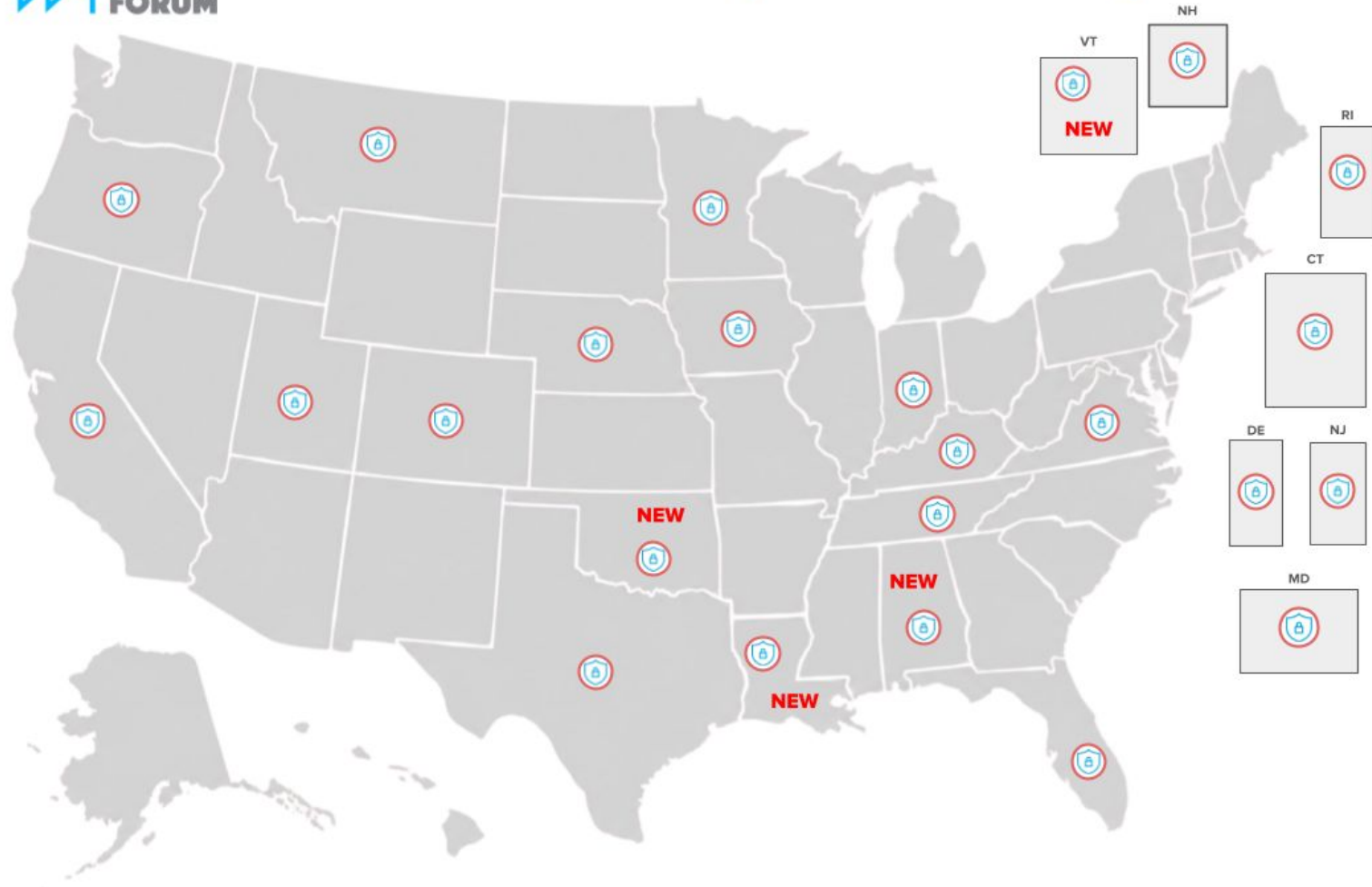
State AI, Privacy, and Youth Laws



KEY

- | | | | |
|---------------|-----------------------|----------------|---------------|
| AI - Chatbots | Biometrics | Data Brokers | Youth Privacy |
| AI - Other | Comprehensive Privacy | Health Privacy | Youth Safety |

State Comprehensive Privacy Laws



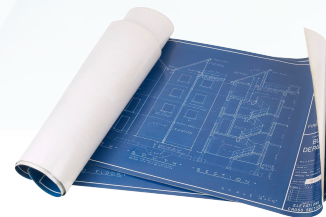
What Makes a Privacy Law “Comprehensive”?

- **Scope**
 - Broadly applicable, non-sectoral, technology-neutral
- **Building Blocks**
 - **Covered entities**
 - Controllers & Processors
 - **Covered data**
 - Personal Data and Sensitive Data
 - **Individual Rights**
 - Access, Correction, Deletion, Portability, Opt-out & More
 - **Business obligations**
 - Transparency, Data Minimization, Oversight, Data Security, Non-discrimination, Non-retaliation, & Data Protection Assessments



Comprehensive Privacy As a Foundation

- **Flexible & Adaptable**
- **Constantly Evolving**
 - 13 states have already amended their laws since passage
 - California, Colorado, and Florida finalized regulations; New Jersey in progress
- **Legislative Trends**
 - Increasing applicability
 - Expanding scope of sensitive data
 - New bans on selling sensitive data
 - Heightened protections for minors, biometric data
 - New and expanded consumer rights
 - Data minimization



Two Competing Models

California Consumer Privacy Act (CCPA)

- Enacted in 2018
- Updated in 2020 by the California Privacy Rights Act (CPRA)
- California Privacy Protection Agency (CalPrivacy) adding new rules through regulations
 - Initial regulations March 2023
 - New regulations on ADMT, risk assessments, and cybersecurity audits October 2025.

Washington Privacy Act (WPA) Framework

- Repeatedly introduced in Washington
- Never enacted but became model framework for other states
- Laws share key definitions and common framework but vary significantly in scope, individual rights, and business obligations
- New laws/bills identified by similarity (Virginia-style, Connecticut-style, Maryland-style)

<u>CCPA</u>		<u>WPA Framework</u>
Enforcement	AG and CPPA share authority	Enforcement solely by AGs
Sensitive Data	'Opt-out'	'Opt-in'
Rulemaking	Broad authority e.g., AI, Risk Assessments, Data Minimization, etc	None Exceptions: Colorado, Florida, New Jersey
Scope of Personal Data	Applies to Employee and B2B Data	Only covers 'personal data' in consumer context
Terms	Unique: Business, Service Provider, Contractor, Third Party	Borrowed: Controller, Processor, Data Protection Assessments
Private Right of Action	Narrow, for Data Breaches	None

Scope — Covered Entities

Who's Covered?

Persons that conduct business in the state or produce products/services targeted to residents and either—

- Control or process the personal data of at least **100K** residents, or
- Control or process the personal data of at least **25K** residents and derive more than **20%** gross revenue from selling personal data

Responsibilities are typically allocated by role—

- **Controller:** An individual/legal entity who alone or jointly with others determines the purpose and means of processing personal data.
- **Processor:** An individual/legal entity who processes personal data on behalf of a controller.

Who Isn't Covered?

- Small Businesses
 - Minnesota, Nebraska, Texas exclude SBA-defined small businesses
- Government Entities
- Nonprofits*
- Institutions of Higher Education*
- Entities Subject to Other Privacy Laws ('Entity-level exemptions')
 - GLBA, HIPAA, FCRA, FERPA

Scope — Covered Data

What's Covered?

Applies to processing of **personal data**—any information linked or reasonably linkable to an identified or identifiable individual [or device].

Heightened protections for **sensitive data**—

- Personal data revealing certain characteristics [racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, citizenship or immigration status]
- Biometric or genetic data processed for unique identification
- Personal data collected from a known child
- Precise geolocation data (1,750' or 1,850')

What Isn't Covered?

- Publicly Available Information
- Deidentified Data*
- Pseudonymous Data* ↔ Limited Exceptions
- Data subject to other privacy laws ('Data-level exemptions')
- Employee data

Exceptions

Broad carve outs for common business activities—

- Complying with legal obligations of law enforcement requests;
- Providing a requested product or service;
- Preventing security threats or illegal activity;
- Public interest research.

Individual Rights

Core Rights

- **Confirm** whether processing is taking place and **access** personal data being processed
- **Correct** inaccurate personal data
- Obtain personal data in a **portable** format
- Require that a controller **delete** personal data in their possession

Consent and Opt-out

- Opt-in for processing sensitive data
- Opt-out of processing for—
 - **Targeted advertising**
 - **Sale** of personal data (disclosure for monetary or other valuable consideration)
 - **Profiling** in furtherance of automated decisions with legal or similarly significant effects
- Exercise opt-outs on a default basis via **authorized agents** and **universal opt-out mechanisms** (UOOMs) for targeted advertising and sale

Business Obligations

- **Transparency:** Disclose data collection and processing activities
- **Data Minimization:** Don't process data for undisclosed and incompatible purposes unless you obtain affirmative consent
- **Service Provider Oversight:** Ensure that any downstream processing is carried out pursuant to a binding contract
- **Data Security:** Maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data
- **Non-discrimination:** Don't process data in violation of laws prohibiting unlawful discrimination
- **Non-retaliation:** Don't raise the cost of or degrade a service because an individual exercised one of their data rights
- **Data Protection Assessments:** Conduct and document a review of certain processing activities that identifies the activity's benefit, risks, and safeguard that can mitigate the risks

Legislative Trends

- States Tinkering with Applicability Thresholds
- Expanding Scope of Sensitive Data
- Data Minimization
- Heightened Protections
- New and Expanded Consumer Rights

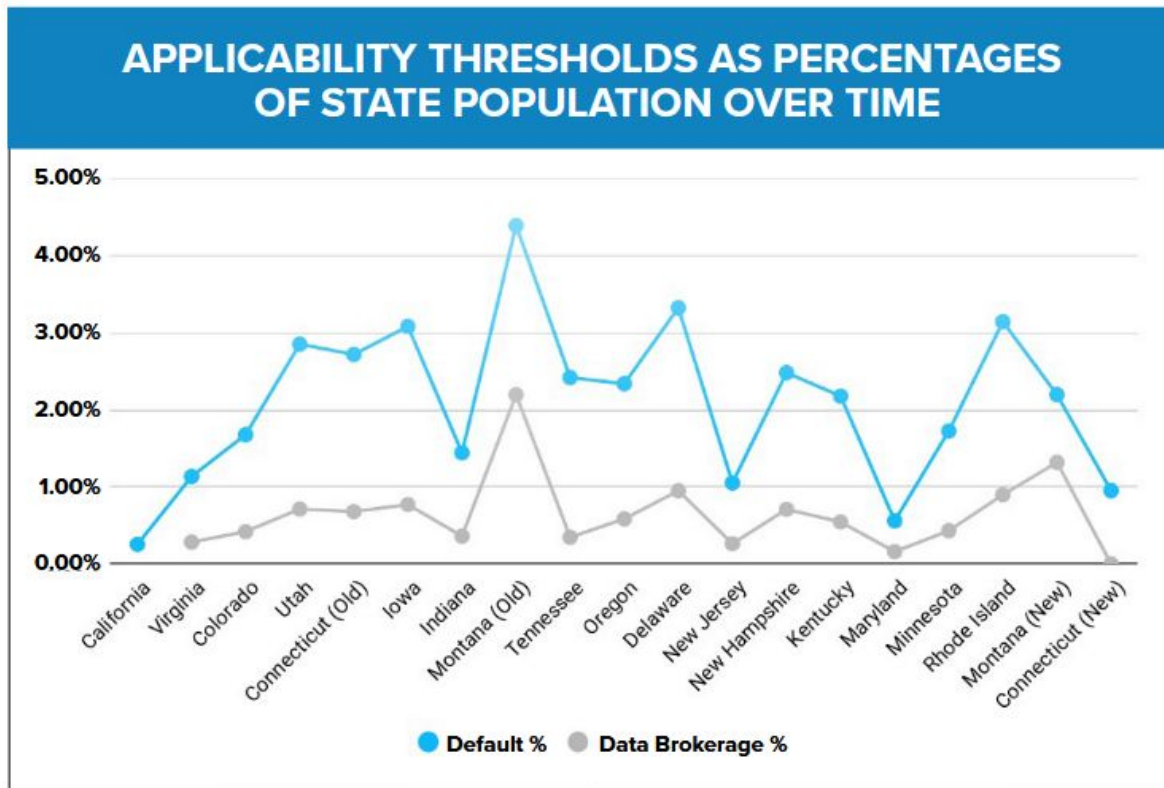


States Tinkering with Applicability Thresholds

	Population (Approx.)	High / Low Thresholds	Percents	Year of Enactment
Colorado	5.96 million	100,000 / 25,000	1.72% / 0.43%	2021
Connecticut	3.68 million	100,000 / 25,000	2.76% / 0.69%	2023
New Jersey	9.50 million	100,000 / 25,000	1.08% / 0.27%	2024
New Hampshire	1.41 million	35,000 / 10,000	2.49% / 0.71%	2024
Maryland	6.26 million	35,000 / 10,000	0.56% / 0.16%	2024
Rhode Island	1.11 million	35,000 / 10,000	3.19% / 0.91%	2024
Connecticut (NEW)	3.68 million	35,000 / 0	0.95% / 0%	2025
Montana (NEW)	1.14 million	25,000 / 15,000	2.20% / 1.32%	2025

→ 2026 amendments continued lowering thresholds

States Tinkering with Applicability Thresholds



**+ Removing
entity-level
exemptions**

Figure 2. Applicability Thresholds as Percentages of State Population

Expanding Scope of Sensitive Data

CATEGORY	SENSITIVE DATA ELEMENTS: PERSONAL DATA THAT REVEALS, INCLUDES, OR IS—	STATES
Health	Personal information collected and analyzed concerning a consumer's health	CA
	Mental or physical health diagnosis	VA, IA, TN, TX, KY, NE
	Mental or physical health diagnosis made by a healthcare provider	IN
	Mental or physical health condition or diagnosis	CO, MT, OR, NH, MN
	Mental or physical health condition or diagnosis (including pregnancy)	DE
	Mental or physical health condition, diagnosis, disability or treatment	CT
	Mental or physical health condition, treatment, or diagnosis	NJ
	Information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a healthcare professional	UT
	Consumer health data (defined term)	CT, MD

Health Data Expanding: Increasingly covering inferences

- E.g., **any** personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis

Trend: Banning the sale of sensitive data

- All Sensitive Data
 - Maryland & New Jersey
- Minor's Personal Data
 - Maryland (u18), Oregon (u16), New Hampshire (u13)
- Precise Location Data
 - Connecticut, Oregon, & Virginia

Data Minimization in the Spotlight

- **FIP:** Do not collect or retain personal information beyond what is adequate, relevant, and proportionate to accomplish a specified, lawful purpose
- Privacy advocates consistently focused on excessive data collection
→ Increased calls for “substantive” protections, particularly meaningful data minimization
- **Emergence of 3 distinct standards in state comprehensive privacy laws:**
 - ‘Procedural’ data minimization (18 of the state laws)
 - ‘Substantive’ data minimization (Maryland)
 - ‘Reasonable Expectations’ -based purpose limitation (California)

Competing Standards

- **Procedural:** Limit the collection of personal data to what is reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer, and get consent for incompatible secondary uses.
- **Substantive:** Limit the collection of personal data to what is reasonably necessary to provide or maintain a specific product or service requested by the consumer to whom the data pertains
- **Reasonable Expectations:** The purposes for which personal information are collected or processed shall be consistent with the reasonable expectations of the consumer whose personal information is collected or processed.

Heightened Protections

State laws increasingly including heightened protections for specific sub-categories of sensitive data:

- Adolescents' personal data
- Consumer health
- Biometrics
- Location

The real “patchwork”?

Approaches to Teens' Privacy

1. Changing Opt-outs to Opt-ins for Teens

STATE	PROTECTED AGES	SALE	TARGETED ADVERTISING	PROFILING
California	Under 16	X	X	
Montana	Under 16	X	X	X
Oregon	Under 16	X	X	X
Delaware	Under 18	X	X	
New Jersey	Under 17	X	X	X
New Hampshire	Under 16	X	X	
Minnesota	Under 17	X	X	

2. Duty of Care

- Connecticut, Colorado, Montana
- Protections for minors under 18; duty to protect from heightened risk of harm; design restrictions; data use limitations

3. Bans

Maryland prohibits—

- Processing an individual's personal data for **targeted advertising** if the controller **knew or should have known** that the individual was **under the age of 18**
- Selling an individual's personal data if the controller **knew or should have known** that the individual was **under the age of 18**

Note: “should have known” differs from “willfully disregards” language seen in other states.

Consumer Health - Scope

- Connecticut's 2023 amendments (SB 3) added protections for “consumer health data” (new category of sensitive data); later included in Maryland's law as well
- Definitions—
 - Connecticut: Personal data that a controller **uses to identify** a consumer's physical or mental health **condition or diagnosis**, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data
 - Maryland: Personal data that a controller **uses to identify** a consumer's physical or mental health **status** [including data related to gender-affirming treatment or reproductive or sexual health care].

Consumer Health - Obligations

- Consumer health data protections apply more broadly than the rest of the law
- Consumer health data controllers cannot
 - Provide employees or contractors with access to consumer health data unless that recipient is subject to a statutory or contractual ***duty of confidentiality***;
 - Provide processors with consumer health data unless the contractor is bound by a processor agreement;
 - ***Geofence*** mental, reproductive, or sexual health facilities (within a boundary of 1,750 feet) for identifying, tracking, or collecting data or sending notifications to an individual about their consumer health data; or
 - ***Sell or offer to sell consumer health data*** without obtaining opt-in consent.

New and Expanded Consumer Rights

- States continue to tinker with consumer rights
- Right to know third party recipients of one's personal data (Oregon, Delaware, Maryland, Minnesota, Connecticut)
 - Differences in terms of **level of specificity** (specific third parties v. categories of third parties) and **personalization** (your personal data or any personal data).
- Right to contest adverse profiling decisions (Minnesota)
 - Ability to **question** the result of the profiling, be informed of **the reason** that the profiling resulted in the decision and actions to secure a different decision, **review** the personal data used in the profiling, and, if using inaccurate data, have the data corrected and the decision reevaluated.
 - Narrower version of this right in Connecticut and Vermont
 - California has new ADMT opt-out regulations

State Enforcement Activity

Prior to 2025

- Regular enforcement under UDAP and state sectoral privacy laws
- Limited enforcement of new comprehensive consumer privacy laws
- Some initial CCPA enforcement
 - Sephora, DoorDash, Tilting Point Media

2025 Actions

- **California**
 - **AG:** Healthline Media, SlingTV, Jam City, Disney
 - **CalPrivacy:** Honda, Todd Snyder, Tractor Supply Company, PlayOn Sports, Ford
- **Texas**
 - Allstate (and Arity)
 - Sony; Samsung; LG; Hisense; TCL
- **Florida:** Roku TV
- **Utah:** Snap
- **Kentucky:** Character.ai

State Sectoral Privacy Laws

Consumer Health

- Washington My Health My Data Act
- Nevada SB 370
- Direct-to-Consumer Genetic Testing Laws

Artificial Intelligence

- High-risk decisionmaking
 - Colorado AI Act
- Chatbots
- Generative AI transparency
- Frontier model safety

→ See FPF blog post [From Proposal to Passage: Enacted U.S. AI Laws, 2023–2025](#)

Youth Privacy & Online Safety

- App Store Accountability Acts
 - Texas, Louisiana, Utah
 - Require age verification at the app store level
- Age Appropriate Design Codes
 - California, Maryland, Vermont, Nebraska, South Carolina
- ‘Addictive Feeds’ Laws
 - New York, California
- Other
 - New York Child Data Protection Act
 - California AB 1043 (age signals)

Data Brokers

- Registries
 - Vermont, Texas, Oregon, Nevada
- California Delete Act

→ Active area of legislation

State Privacy Law Resources

REPORT

U.S. LEGISLATION | JUNE 2025

Data Minimization's Substantive Turn

Key Questions & Operational Challenges Posed by New State Privacy Legislation

Data minimization—collecting, using, or retaining personal data only to the extent necessary to accomplish an identified, lawful purpose—is a bedrock principle of privacy and data protection law. State privacy laws have begun to embrace new “substantive” data minimization rules that impose default restrictions on the purposes for which personal data can be collected, used, or shared. This white paper explores this ongoing trend towards substantive data minimization and the unresolved policy implications of this new language.



**FUTURE OF
PRIVACY
FORUM**

REPORT

U.S. LEGISLATION | DECEMBER 2025

Anatomy of a State Comprehensive Privacy Law

Charting the Legislative Landscape

The state privacy landscape continues to evolve year-to-year as laws are enacted, amended, and enforced. This report summarizes that legislative landscape, compares and contrasts the prevailing models for state laws, and identifies the critical commonalities and differences in the laws' components that collectively constitute the “anatomy” of a state comprehensive privacy law.



**FUTURE OF
PRIVACY
FORUM**

ISSUE BRIEF U.S. Policy

NEW

THE BOUNDARIES OF DATA BROKERAGE

AN OVERVIEW OF THE U.S. REGULATORY LANDSCAPE

JULY 2026



**FUTURE OF
PRIVACY
FORUM**

Follow these QR codes for access to a few of my reports.

Thank you! Reach out at jfrancis@fpf.org with any follow-up questions.