The US Consumer Privacy Law Landscape

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

FUTURE OF PRIVACY FORUM

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, plus policy staff in India & Kenya.

FUTURE OF PRIVACY FORUM

FPF Members & Teams

200+ Companies

20+ Civil Society

45+ Academics

50+ Staff & Fellows

FPF Workstreams

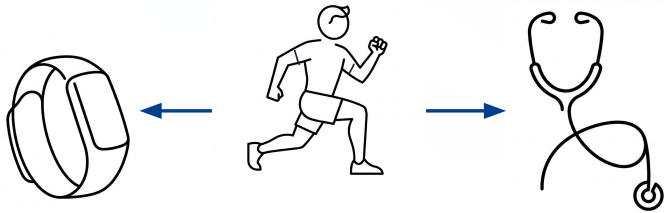
- U.S. Legislation & Regulation
- Youth Privacy & Online Safety
- Ad Practices
- Biometrics
- Health & Wellness
- Mobility & Location
- FPF Center for Artificial Intelligence
- Global Data Protection
  - Europe
  - Asia-Pacific
  - Africa
  - Americas

FUTURE OF PRIVACY FORUM

Personal Data and AI in Healthcare

The Health Data Ecosystem is Diverse

- Traditional health care ecosystem
  - Patients interact with medical professionals in clinics, hospitals, etc
- Consumer health ecosystem
  - Wearables like smart watches collect body-based and biometric data
  - Apps facilitate for prescription drug purchasing, telehealth, tracking bodily functions (e.g., reproductive health)
  - Retail purchases reveal health information
  - Browsing health-related content online feeds into ad ecosystem



FUTURE OF PRIVACY FORUM

Personal Data and AI in Healthcare

Privacy in the Health Ecosystem

- Electronic Health Records
  ➔ HIPAA & State Laws
- Consumer Data
  ➔ State Privacy Laws (sensitive data protections)
- Genetic Data
  ➔ Non-Discrimination Laws; Direct-to-Consumer Genetic Testing Laws

Artificial Intelligence

- Generative AI in Healthcare
  ➔ Limits on AI provision of mental health services; AI Transcription Tools
- Automated Decisionmaking
  ➔ Claims denials without a "human in the loop"

FUTURE OF PRIVACY FORUM

US Consumer Privacy Laws

- **Fragmented Federal Landscape**
- **State Comprehensive Privacy Laws**
  - 23-24 state comprehensive privacy laws
- **Trends**
  - Broadening Applicability
  - Expanding Scope of Sensitive Data
  - Data Minimization
  - Heightened Protections for Biometrics, Health, and Minors
  - New and Expanded Consumer Rights
- **Sectoral Privacy Laws**
  - Biometrics
  - Data Brokers
  - Consumer Health
    - **My Health My Data**
  - Genetic Testing
  - Insurance

FUTURE OF PRIVACY FORUM

Federal Privacy Laws

FUTURE OF PRIVACY FORUM

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)**
    - **Covered Entities** = Health plans, health care clearinghouses, health care providers
    - **Business Associates** = Persons who access PHI to perform certain services on behalf a covered entity
  - **Other laws** address children's privacy (COPPA), financial privacy (GLBA), consumer reports (FCRA), unfair and deceptive trade practices (FTC Act), video records (VPPA), data brokers and foreign adversaries (PADFAA), etc.

FUTURE OF PRIVACY FORUM

FTC Enforcement Actions

- **GoodRx (2023)**
  - Alleged that the company violated the Health Breach Notification Rule (HBNR) and committed an “unfair” trade practice by sharing users’ identifiable health information with third-party advertising platforms without users’ knowledge or consent
  - Further alleged deceptive conduct by presenting a HIPAA compliance certification seal on its webpage
- **BetterHelp (2023)**
  - Alleged that the company was sharing users’ personal information, including hashed email addresses, with advertising partners for retargeting and creating lookalike audiences
- **Premom (2023)**
  - Similar to the GoodRx complaint, alleged that the company violated the HBNR and committed an unfair trade practice by sharing sensitive health information with advertising partners

FUTURE OF PRIVACY FORUM

State Privacy Laws

FUTURE OF PRIVACY FORUM

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

4,400+
BILLS REVIEWED BY FPF

1,400+
BILLS TRACKED BY FPF

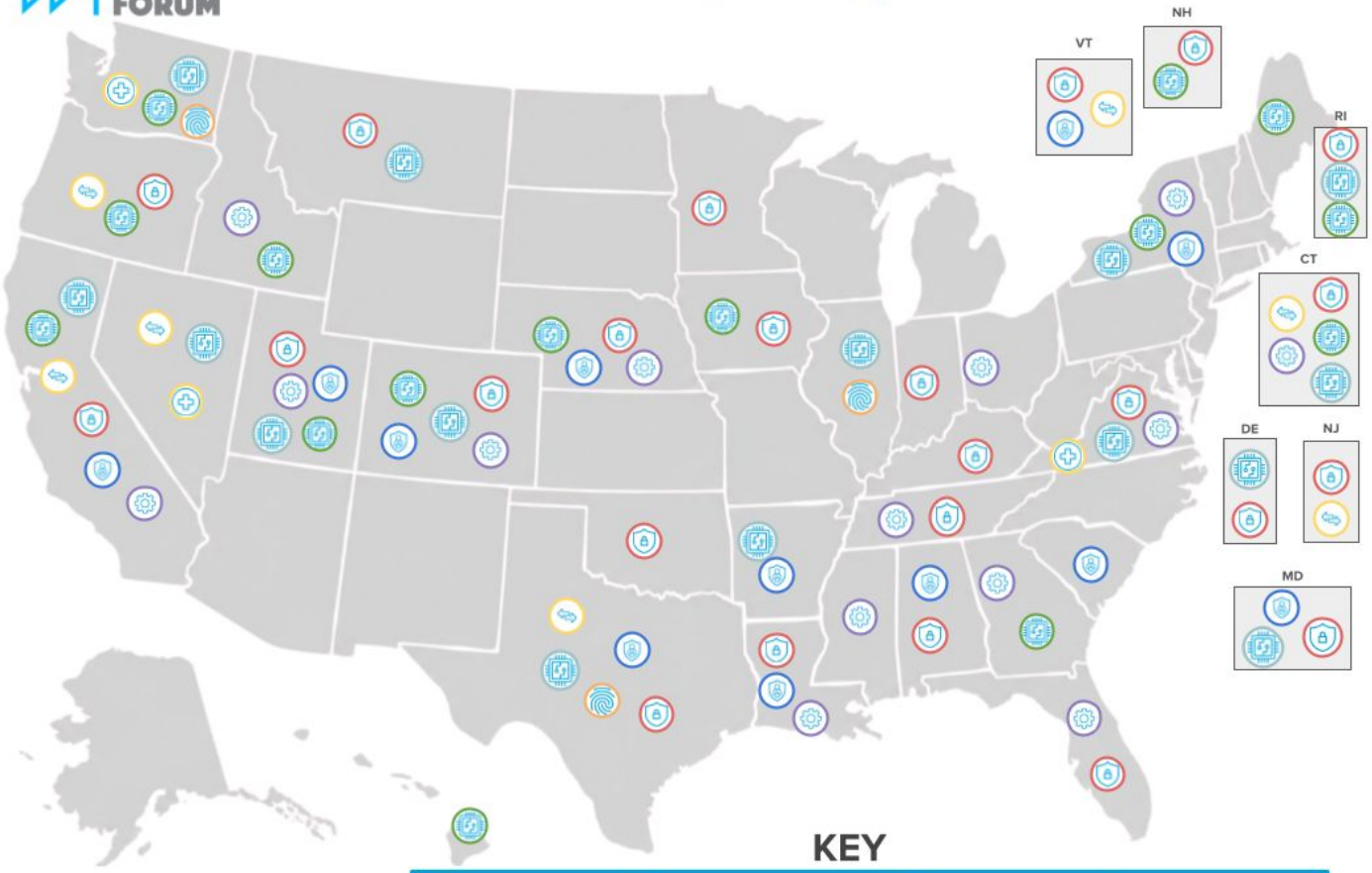
50+
BILLS ENACTED

- 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

FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM

State AI, Privacy, and Youth Laws



KEY

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

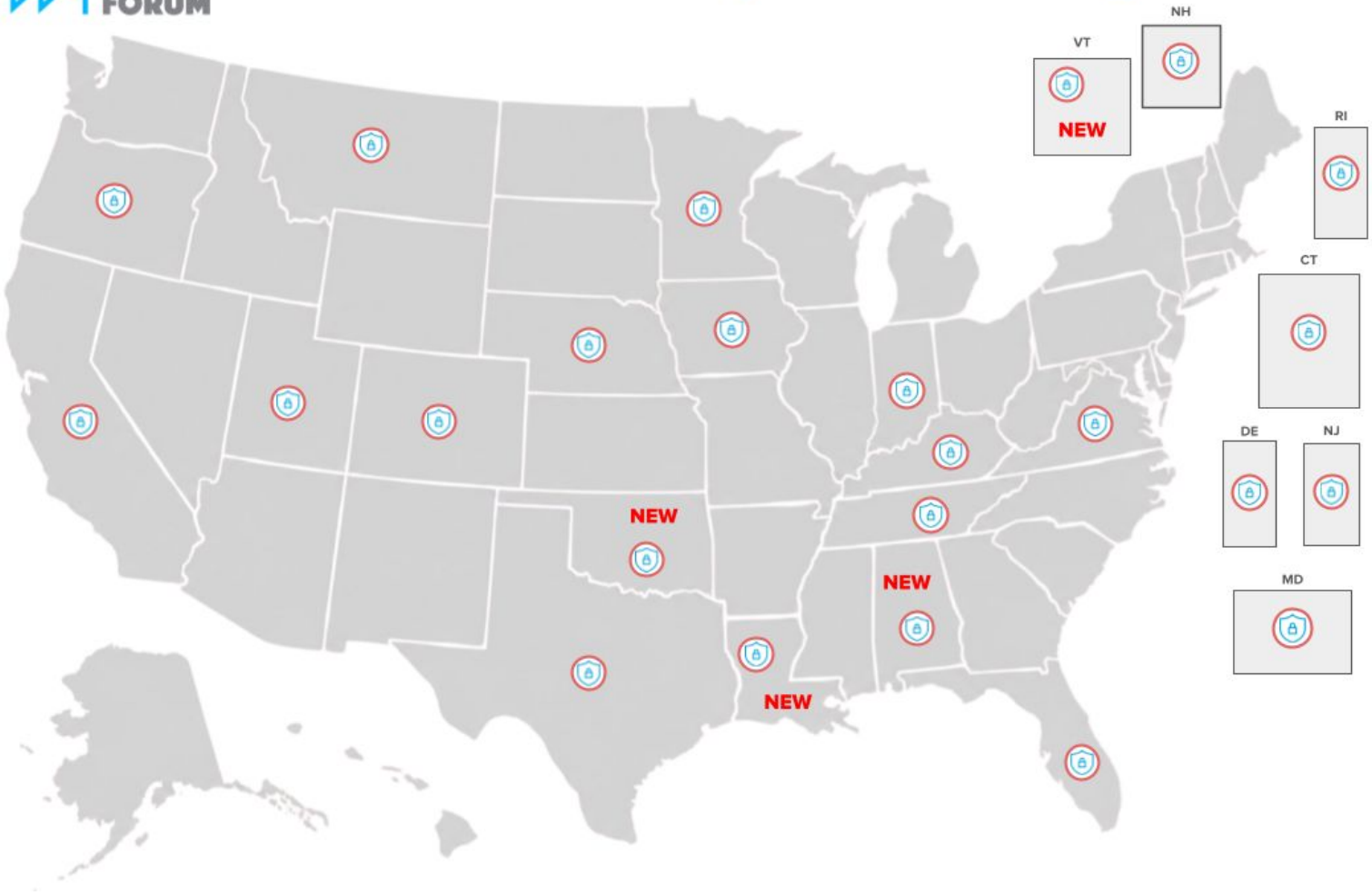
Last updated July 17, 2026

State Comprehensive Privacy Laws

FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM

State Comprehensive Privacy Laws



What Makes a Privacy Law “Comprehensive”?

- **Scope**
  - Broadly applicable, non-sectoral, technology-neutral
- **Constantly Evolving**
  - Regular amendments (13 states)
  - Rulemaking (California, Colorado, Florida, New Jersey)
- **Legislative Trends**
  - Increasing applicability
  - Expanding scope of sensitive data
    - New bans on selling sensitive data
  - Heightened protections for biometrics, health, location, minors
  - Data minimization
  - New and expanded consumer rights

FUTURE OF PRIVACY FORUM

Two Competing Models

California Consumer Privacy Act (CCPA)	Washington Privacy Act (WPA) Framework

• 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.
	• 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)

FUTURE OF PRIVACY FORUM

	CCPA	WPA Framework
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

FUTURE OF PRIVACY FORUM

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
- Government Entities
- Nonprofits*
- Institutions of Higher Education*
- Entities Subject to Other Privacy Laws ('Entity-level exemptions')
  - GLBA, HIPAA, FCRA, FERPA

FUTURE OF PRIVACY FORUM

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') (HIPAA, state health records laws)
- 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.

FUTURE OF PRIVACY FORUM

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

FUTURE OF PRIVACY FORUM

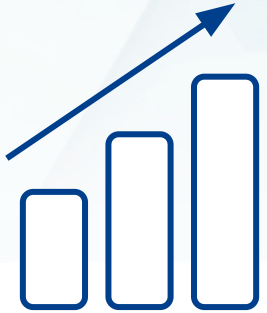
Business Obligations

- **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

FUTURE OF PRIVACY FORUM

Legislative Trends

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



FUTURE OF PRIVACY FORUM

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

FUTURE OF PRIVACY FORUM

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)

FUTURE OF PRIVACY FORUM

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.

FUTURE OF PRIVACY FORUM

CCPA Regulations § 7002: Reasonable Expectations

Enforced in the California DOJ's settlement with publisher Healthline, Inc. in 2025. The AG alleged:

> "Healthline had transmitted article titles referencing current diagnoses of serious diseases, potentially revealing health-related information about readers to third parties [e.g., "Newly Diagnosed with HIV? Important Things to Know."]. This violated the CCPA's 'purpose limitation principle' by disclosing health-related data for two unexpected uses—targeted advertising and third-party inferences based on what a consumer was reading."

FUTURE OF PRIVACY FORUM

CCPA Regulations § 7002: Reasonable Expectations

The publisher earns revenue by displaying advertising on its website, including targeted ads. This practice (sharing PI with advertising providers for the purpose of targeted advertising) was disclosed in the privacy notice.

> "[T]he law provides that invisibly sharing data of a more intimate nature to third parties, briefly alluded to in a privacy policy, may be unlawful when consumers would not expect that to happen. The law further provides that even detailed privacy disclosures regarding other intended uses of data may violate the principle if the disclosed purposes differ substantially from the consumer's reasonable expectations. . . . [E]ven if Healthline's privacy policy discussed targeted advertising briefly, it never mentioned sharing article titles. Nor would consumers see those titles being shared in the digital background. Healthline therefore could not establish that consumers reasonably expected that Healthline would share potentially health-related data, as the purpose limitation principle requires."

FUTURE OF PRIVACY FORUM

Heightened Protections

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

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

FUTURE OF PRIVACY FORUM

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].

FUTURE OF PRIVACY FORUM

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.

FUTURE OF PRIVACY FORUM

New and Expanded 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.

FUTURE OF PRIVACY FORUM

State Sectoral Privacy Laws

FUTURE OF PRIVACY FORUM

State Sectoral Privacy Laws

Consumer Health

- **Washington My Health My Data Act**
- **Nevada SB 370**
- **Virginia Reproductive Privacy Amendment**
- **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, New Jersey
- **Accessible Deletion Mechanisms**
  - California, Connecticut

➔ Active area of legislation

FUTURE OF PRIVACY FORUM

My Health My Data - Scope

- Passed in 2023 in response to *Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022)*
- Structurally similar to a comprehensive privacy law, but limited to ***consumer health data***
  - Personal information that is linked or reasonably linkable to a consumer and that ***identifies the consumer's past, present or future physical or mental health status***.
  - Includes bodily functions, vital signs, symptoms, biometric data, genetic data, precise geolocation information that could reasonably indicate an attempt to acquire or receive health services or supplies, and more.
  - Exclude HIPAA-covered PHI, de-identified data, data used for public research, publicly available information
- Protects Washington residents and persons whose consumer health data is ***collected*** in Washington
  - Collected defined to include "processed" ➔ Broad reach

FUTURE OF PRIVACY FORUM

My Health My Data - Obligations

- Regulated entities prohibited from processing consumer health data unless
  - With consent from the consumer “for a specified purpose”, or
  - Necessary to provide a product or service requested by the consumer
- Separate consent required to share consumer health data (or unless necessary to provide a requested product or service)
- ***Selling*** consumer health data requires “valid authorization,” an even higher standard of consent
- Consumer rights of access, withdrawing consent, and deletion
- Enforcement via Washington Consumer Protection Act
  - AG enforcement and ***private right of action*** (tied to actual damages)

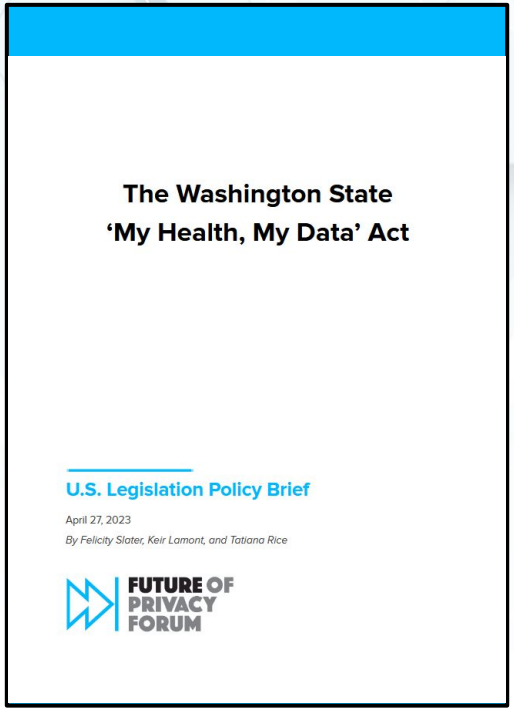
FUTURE OF PRIVACY FORUM

My Health My Data - Litigation

- Very little public litigation despite private right of action.
  - Actual damages v. statutory damages?
- **Maxwell v. Amazon.com Inc** (2:25-cv-00261) (W.D. Wash.)
  - Alleged advertising SDK in third-party apps collected precise geolocation data that could reveal attempts to receive healthcare, absent consent
  - Consolidated with other SDK litigation in *In re Amazon Ads SDK Litigation*, (2:25-cv-00252) (W.D. Wash.) ➔ ultimately dismissed without prejudice
- **K.R. v. 1400 23rd LLC et al.** (2:25-cv-02211) (W.D. Wash.)
  - Cannabis retailer Uncle Ike's accused of using tracking pixels to collect consumer health data (information about appointments and purchases) without valid consent or sufficient disclosure.

FUTURE OF PRIVACY FORUM

State Privacy Law Resources



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

FUTURE OF PRIVACY FORUM

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

FUTURE OF PRIVACY FORUM