Up-Leveling Your Privacy Program To Make Sense of The Latest State Privacy Law Developments

Hanna Abrams, Libbie Canter, Kate Goodloe, Liz Lyons

May 8, 2025

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON
LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

www.cov.com

Presenters

Hanna Abrams
Maryland Office of the Attorney General

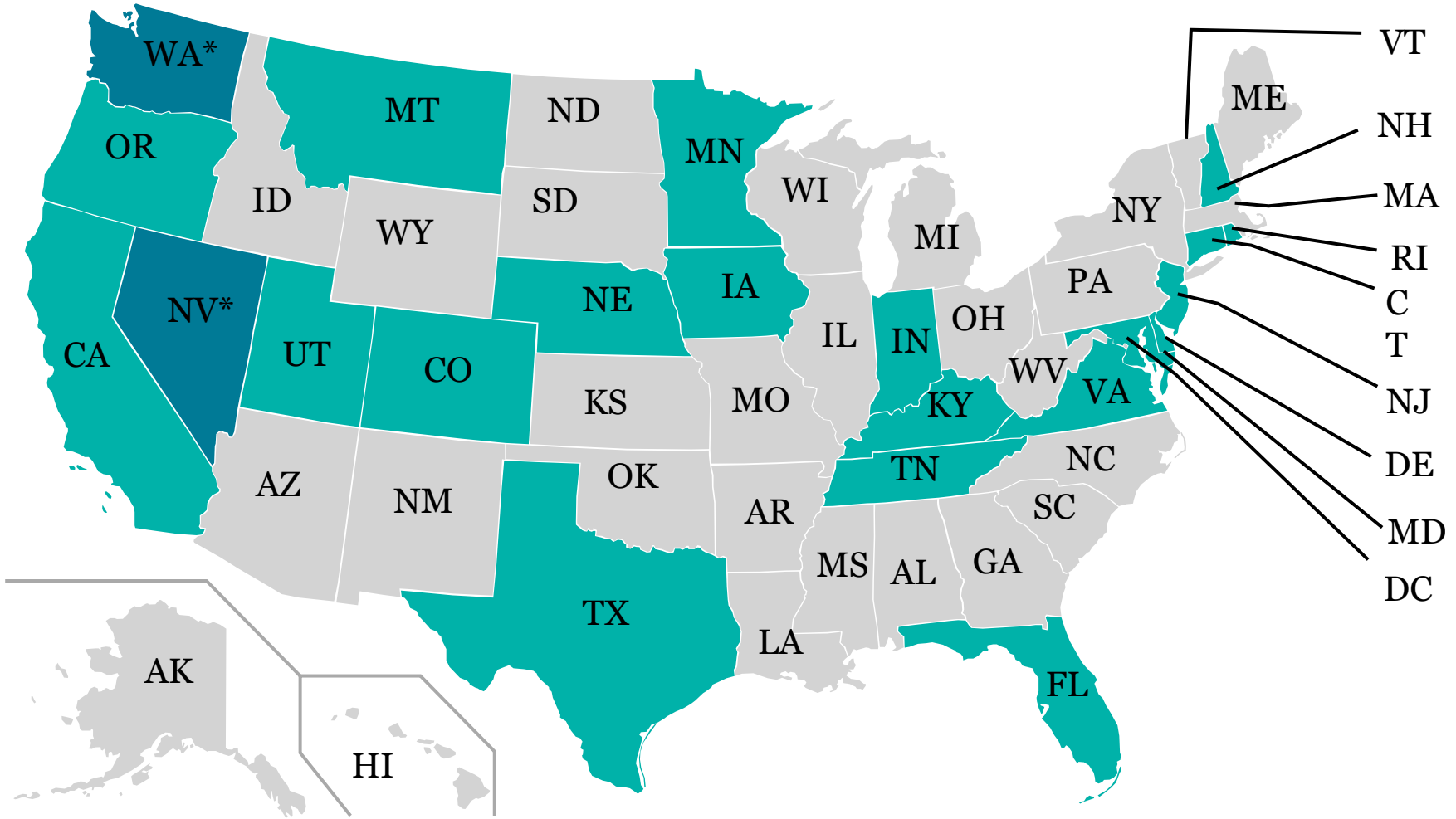
Libbie Canter
Covington & Burling LLP

Kate Goodloe
Business Software Alliance

Liz Lyons
HP

Overview of State of the States

20 States With Enacted Comprehensive Privacy Laws



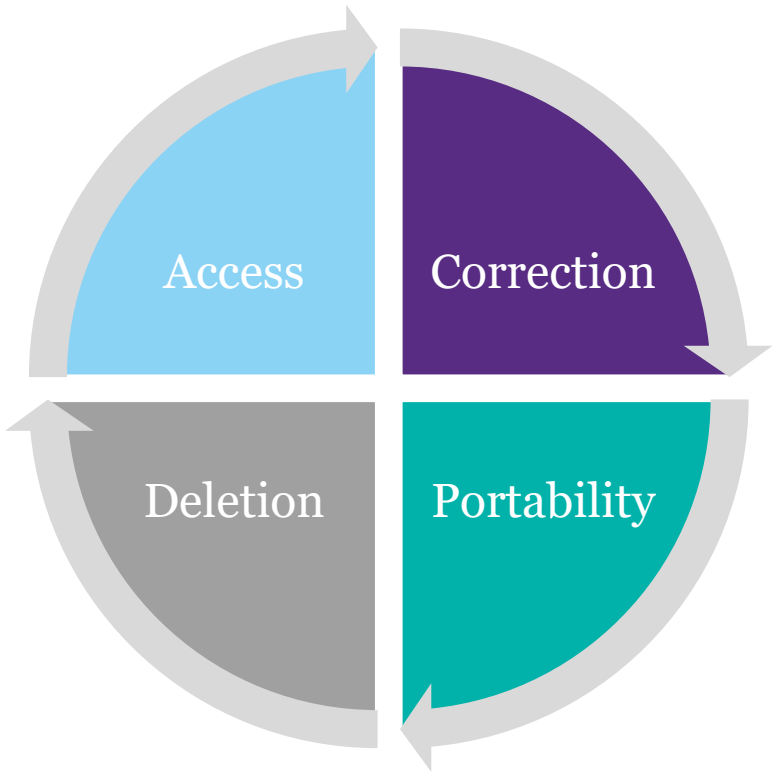
**WA and NV have enacted separate consumer health data laws; NV also has certain other protections for sales of personal data.*

Key Controller Obligations

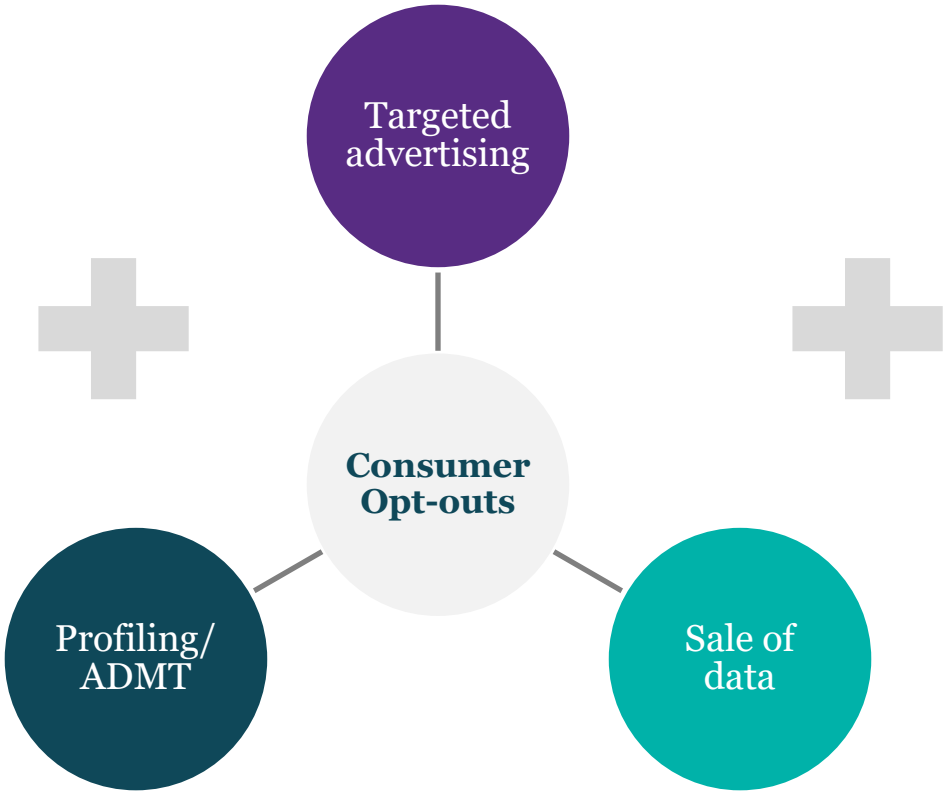
- Privacy Notices
- Data Subject Rights (including opt out rights)
- Minimization and Retention
- Service Providers and Contractor Terms
- Protections for Sensitive Data (including for minors)
- Reasonable Security Procedures and Practices
- Data Protection Assessments
- Discrimination/ Retaliation

Data Subject Rights

GDPR-Like Rights



Opt-Out Rights



Withdraw Consent or Opt-Out Rights for Sensitive Data

Key Processor Obligations

- Duty of Confidentiality
- Reasonable Security Measures
- Data Return or Deletion
- Consumer Request Compliance
- Subcontractor Compliance
- Comply with Reasonable Assessments
- Provide Relevant Information for Compliance

Categories of State Privacy Laws

"Fewer Substantive Obligations"

- Utah
- Iowa

"Baseline Approach"

- Virginia
- Indiana
- Kentucky
- Tennessee
- Florida
- Texas
- Nebraska
- Rhode Island*

"More Substantive Obligations"

- Colorado
- Connecticut
- New Hampshire
- New Jersey
- Montana
- Delaware
- Oregon

"Outliers"

- California
- Maryland
- Minnesota
- Washington and Nevada consumer health data laws

Areas of Divergence

Scope

- California law applies to employee and B2B data
- Variation in exemptions, including for financial institutions, non-profits, etc.

Sensitive Data

- Variation in definitions of sensitive data
- Variation in opt-in versus opt-out approach

Children & Minors

- Most states treat data about children under 13 as sensitive
- Some states impose additional requirements for children 13-16 (e.g,. opt-in to sale of data)

Opt-Out Rights

- Variation in scope of rights, including sale definition
- Variation in required mechanisms for consumers to opt out (e.g., global opt-out preference signals)

DPIAs

- Most state laws are not prescriptive
- Colorado rules including detailed requirements (e.g., profiling) and ongoing California rulemaking

Other

- Oregon and Minnesota give consumers right to obtain a list of specific third parties to whom controllers disclose a consumer's personal data.
- Financial incentive/loyalty program requirements

What To Expect for 2025 and 2026

Effective Dates

Timeline	
January 1, 2023	California (CPRA amending CCPA), Virginia
July 1, 2023	Colorado, Connecticut
December 31, 2023	Utah
July 1, 2024	Florida, Texas, Oregon
October 1, 2024	Montana
January 1, 2025	Delaware, Iowa, Nebraska, New Hampshire
January 15, 2025	New Jersey
July 1, 2025	Tennessee
July 31, 2025	Minnesota
October 1, 2025	Maryland
January 1, 2026	Indiana, Kentucky, Rhode Island

New Consortium of Privacy Regulators

Eight state regulators have announced a new consortium to collaborate on implementation and enforcement of their privacy laws.

Members include the California Privacy Protection Agency and state Attorneys General from California, Colorado, Connecticut, Delaware, Indiana, New Jersey, and Oregon

Cure Periods

Timeline		
State	**Cure Period**	**Expiration Date**
Delaware, New Hampshire	60 days	December 31, 2025
Oregon	30 days	January 1, 2026
Minnesota	30 days	January 31, 2026
New Jersey	30 days	July 1, 2026
Montana	60 days	April 1, 2026
Maryland	60 days	April 1, 2027
Nebraska, Texas, Utah, Virginia (and, soon, Kentucky and Indiana)	30 days	No Sunset
Florida	45 days	No Sunset
Tennessee	60 days	No Sunset
Iowa	90 days	No Sunset

Ongoing Enforcement

UPDATED ENFORCEMENT REPORT PURSUANT TO CONNECTICUT DATA PRIVACY ACT, CONN. GEN. STAT. § 42-515, ET SEQ.

April 17, 2025

January 13, 2025 | Press Release

Attorney General Ken Paxton Sues All-state and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies

CPPA Brings Enforcement Action Against Florida Data Broker

CALIFORNIA PRIVACY PROTECTION AGENCY
ENFORCEMENT DIVISION

ENFORCEMENT ADVISORY NO. 2024-01

APPLYING DATA MINIMIZATION TO CONSUMER REQUESTS

Sephora pays $1.2 million to settle a California suit accusing it of selling customer data without telling them

Up-Leveling Your Privacy Program for Latest Developments

Policy and Procedure Requirements

Tennessee Approach

- Affirmative defense if controller or processor has written privacy policy that reasonably conforms to NIST Privacy Framework

Minnesota Approach

- Minnesota requires controllers to document and maintain a description of policies and procedures adopted to comply with the state's privacy law
- The description must include, where applicable:
  - The name and contact information for the controller's chief privacy officer.
  - Policies and procedures designed to reflect requirements of law in the design of the controller's system, to provide personal data to a consumer as required by the law, to maintain reasonable security practices, to limit the collection of personal data to what is adequate, reasonable, and reasonably necessary, to prevent retention of personal data that is no longer relevant and reasonably necessary, and to identify and remediate violations of the law.

Data Security

Majority Approach:

- Requires reasonable measures to protect data. For example:
  - Virginia: Controllers must establish, implement, and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue.

Minnesota:

- Reasonable security practices to include maintenance of an inventory of data that must be managed to exercise controller responsibilities

CA Cyber Audit Rulemaking:

- Must complete a cyber audit if processing presents "significant risk" to consumers' security
- Audits must be completed using an independent auditor
- Prescriptive list of cyber audit requirements. For example, network monitoring and defenses, antivirus and antimalware, incident response, and information assets inventory and management
- Submission of notice of compliance to CPPA

Privacy Notices

"[C]ommon deficiencies identified in [privacy] notices included:

- **Inadequate disclosures** (e.g., failure to sufficiently inform Oregon consumers about their rights under the law, specifically the list of third parties their data has been sold to);
- **Confusing privacy notices** (e.g., notices that are not clear or accessible to the average consumer);
  - For example: notices that name one or two states in the "your state rights" section but not Oregon, giving consumers the impression that privacy rights are only available to people who live in those named states.
- **Lacking or burdensome rights mechanisms** (e.g., failure to include a clear and conspicuous link to a webpage enabling consumers to opt out, request their privacy rights, or inappropriately difficult authentication requirements)."

Enforcement Report: The Oregon Consumer Privacy Act (2024), The First Six Months

Data Minimization

Majority Approach

- Controllers may not process personal data for purposes that are not reasonably necessary to or compatible with the *disclosed* purposes for which such personal data is processed, as *disclosed* to the consumer, absent consent
- Law does not restrict controller's ability to conduct internal research to develop or improve products or services or perform internal operations aligned with expectations of consumer

California Approach

- Absent consent, business's processing of personal information must be reasonably necessary and proportionate to achieve:
  1. purposes for which data was collected (and consistent with reasonable expectations of consumer, taking into account the specificity and prominence of disclosures to the consumer); or
  2. another disclosed purpose compatible with the context.

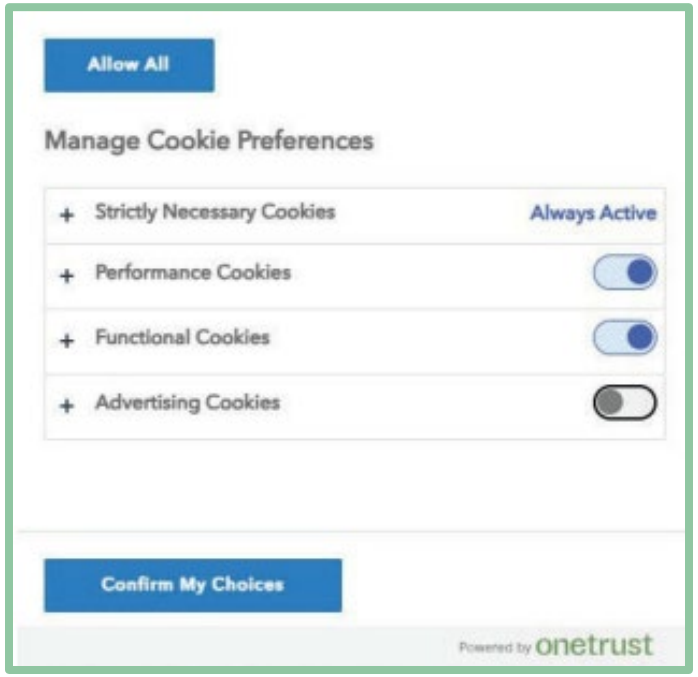
Maryland Approach

- Maryland requires controllers to limit their collection of personal data to *what is necessary and proportionate to provide or maintain a specific product or service* requested by a consumer, as opposed to the purposes listed in their privacy notices, with heightened standard for sensitive personal data.
- Law does not restrict controller's ability to perform internal operations aligned with expectations of consumer

Dark Patterns & Efficacy of Opt Out Rights

One Step to Opt-In: "Allow All"

Two steps to Opt-Out: Toggle + "Confirm My Choices



"Dark pattern" means a user interface designed or manipulated with the ***substantial effect*** *of* ***subverting or impairing user autonomy, decisionmaking, or choice****, as further defined by regulation.*

Sensitive Data Requirements

- Increasing Variation in Scope of Sensitive Data: State privacy laws increasingly recognize a broad range of personal information as sensitive.
- Variation in Protections:
  - States vary in whether businesses must obtain opt-in consent or allow opt-out options for processing.
  - **Maryland** prohibits sale of sensitive data.
  - Consumer health privacy laws (e.g., **Washington**, **Nevada**) require HIPAA-like authorization to sell consumer health data.
- Additional Disclosures May Be Required: **Texas** requires businesses selling sensitive data to include a disclosure: "NOTICE: We may sell your sensitive personal data." In January 2025, Texas AG filed a complaint against Allstate for failing to provide required notices and disclosures.
- Stricter Data Minimization Standard: **Maryland** requires controllers to limit their collection of sensitive personal data to *what is strictly necessary* to provide a product or service.
- Additional Protections for Minors: For example, **Maryland** treats the data of a "known child" as sensitive, defined as someone under 13 where a business has actual knowledge or willfully disregards their age – stricter than states with no defined age threshold.

Profiling and Automated-Decision Making

"Profiling in furtherance of decisions that produce ***legal or similarly significant effects*** concerning the consumer"

-Majority approach to opt-out rights

"***Solely automated*** processing performed on personal information to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements"

- Majority definition of profiling

- **Colorado** rules introduce rights with respect to human reviewed automated processing, with more detailed DPIA expectations for profiling
- **Minnesota** provides an additional right for the consumer to *question the result of profiling* in furtherance of decisions that produce legal or similarly significant effects, to be informed of the reason profiling resulted in decision, to review personal data used in profiling, and to correct personal data and have the profiling decision reevaluated if inaccurate data was used.
- **California** has ongoing rulemaking for additional rights for automated decision-making, defined expansively.
- **Maryland** requires controllers to conduct an *assessment for each algorithm that is used.*

Predictions for the Future

State Privacy Law Predictions

New Legislation	The pace of state legislation slowed in 2025 for comprehensive privacy laws, although states are adopting other kinds of privacy bills and amending existing bills.
Rulemakings	A small number of states have express rulemaking authority. California has a proceeding to adopt rules related to cyber audits, risk assessments, and automated decision-making.
Enforcement	Many states seem poised to enforce their new privacy authorities and greater resources to enforce existing consumer protection and privacy frameworks.

Questions?