



McDermott
Will & Emery

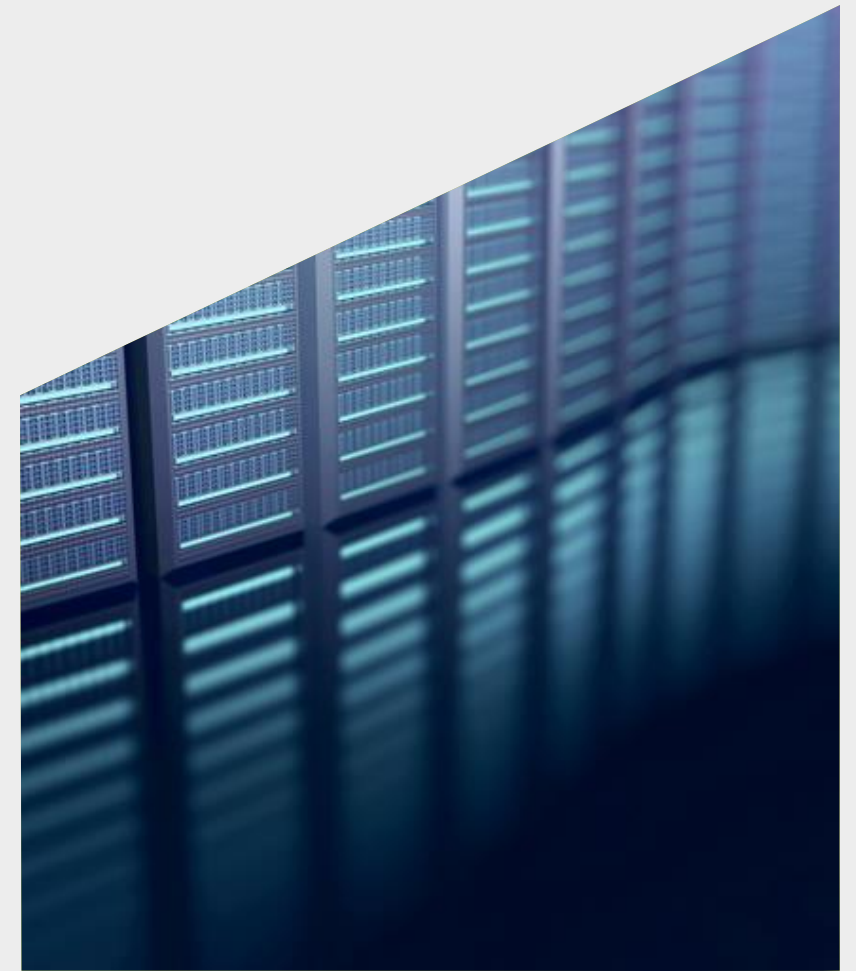


COMING SOON TO A STATE NEAR YOU:

Evolving US Privacy Requirements &
Practical Tips

September 14, 2023

[mwe.com](https://www.mwe.com)

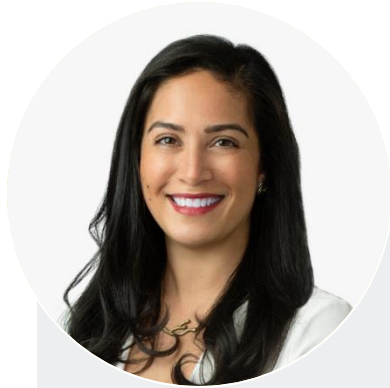


SPEAKERS



ELLIOT GOLDING

McDermott Will & Emery
Partner
egolding@mwe.com



AMY PIMENTEL

McDermott Will & Emery
Partner
apimentel@mwe.com



MAUREEN HERNBERG

McKinsey
Privacy Compliance
maureen_hernberg@
mckinsey.com



JOHN VAUGHAN

Verily Life Sciences
Lead Product Counsel
jtvaughan@verily.com



AGENDA

- Overall 2023 US Landscape
- Creating An Action Plan
- Thank You / Questions

OVERALL 2023 US LANDSCAPE



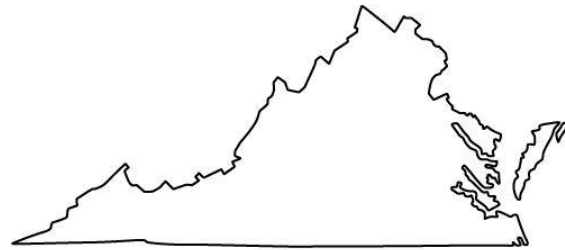
OPERATIONAL IMPACT & ENFORCEMENT

- Aggressive regulators can and will enforce laws
 - In most states, the AG is the primary regulator empowered to enforce these laws
 - In CA, the California Privacy Protection Agency (CPPA) also has this authority
 - In CO, District Attorneys also has this authority
 - AGs can issue **injunctions** and bring civil suits with **penalties** of several thousand dollars per violation
 - Increased **regulatory risk** in exposing other areas of the business
 - **CA Sephora case**: Alleged violation of CCPA resulted in \$1.2 million settlement, requirement to send regular compliance reports to AG
 - CA AG also posted enforcement examples involving health/financial companies
- Colorado's law came into effect July 1, 2023, and the AG has already **published a press release** and **begun a mailing campaign**
- California and Colorado both invite consumers to report potential violations, **enabling broad enforcement sweeps**
- Responding to enforcement is **time consuming**
 - Allegation may require internal investigation, comprehensive plan, PR response
 - Human cost in responding to:
 - Written requests (e.g., CIDs)
 - Full audits
 - Corrective action plans

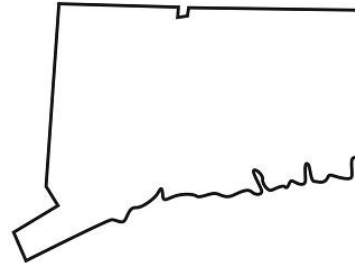
US STATE CONSUMER PRIVACY LAWS IN 2023



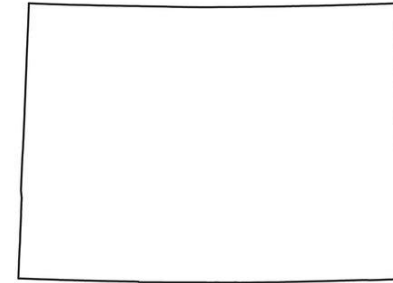
California*
January 1, 2023



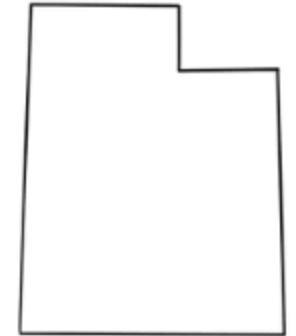
Virginia
January 1, 2023



Connecticut
July 1, 2023



Colorado**
July 1, 2023



Utah
December 31, 2023

Indiana, Iowa, Florida, Montana, Oregon, Tennessee and Texas each passed privacy laws in 2023 which come into effect between July 1, 2024 and January 1, 2026.

**California did not enact not a new law; CPRA amendments took effect*

**** Washington law discussed later*

ENTITY APPLICABILITY

Revenue
OR
Processing

Revenue
AND
Processing

All apply to for-profit entities *except* CO/WA applies to nonprofits

Processing

California

\$25M annually

OR

Buy/sell/share data of
100k residents
annually

/

>50% revenue from
selling/sharing

Utah

\$25M annually

AND

Processes data of
100k residents
annually

/

>50% revenue from
selling & processes
data of 25k residents

Virginia

Processes data of
100k residents
annually

/

>50% revenue
from selling &
processes data of
25k residents

Colorado

Processes data of
100k residents
annually

/

Sells data for
money/discount &
processes data of
25k residents

Connecticut

Processes data of
100k residents
annually

/

>25% revenue
from selling &
processes data of
25k residents

KEY ENTITY EXEMPTIONS

1. Covered entities and business associates under **HIPAA**
 - **Exception:** CA, CO, WA (data only)
2. Financial institutions subject to **GLBA**
 - **Exception:** CA, WA (data only)
3. Nonprofits
 - **Exception:** CO, WA

OTHER EXEMPTIONS

Data subjects

- Except in CA, these laws are only applicable to consumers acting in an individual or household context
 - Not in scope:
 - Employees
 - Job applicants
 - B2B contacts

Data types

- Data regulated by many federal regimes also exempted:
 - e.g., FCRA, FERPA*, COPPA*
 - **Note:** An entity is not always exempt just because it handles these types of data

**No specific exemptions under California law*

KEY REQUIREMENTS UNDER NEW LAWS



Privacy policies (all states)



Contracting requirements (all states)



Privacy rights (all states)



Training



Governance (PIAs, Cyber Assessments)

STATE HEALTH DATA REQUIREMENTS

- Connecticut and New York have laws already in effect that control the processing of health information.
 - Nevada and Washington each passed similar laws effective March 31, 2024.
- The state consumer privacy laws also include heightened requirements for Sensitive Data, which generally includes Health Data.
- While most privacy and health data laws rely exclusively on regulators for enforcement, Washington's My Health My Data Act also creates a private right of action.

STATE HEALTH DATA REQUIREMENTS

- These laws control the processing and disclosure of Health Information collected by products targeted at residents and collected within the state from all individuals.
 - Geofencing of health care facilities is generally prohibited under all of these laws
 - CT, NV, WA require either: (1) specific consent or (2) a product or service for the consumer requiring the processing of consumer health data, prior to processing consumer health data
 - CT, NV, WA require specific consent prior to selling (or offering to sell) consumer health data
 - NV, WA require that regulated entities maintain a separate consumer health data privacy policy

CREATING AN ACTION PLAN



BUILDING A COMPLIANCE PROGRAM

- **Workstream #1:** Info gathering and scoping/harmonization
- **Workstream #2:** Create data inventories/maps (if applicable)
- **Workstream #3:** Update external-facing privacy policy(ies)
- **Workstream #4:** Create/update data subject rights (“DSR”) procedures
- **Workstream #5:** Create/update vendor/data recipient contracting program
- **Workstream #6:** Update governance, internal documentation, training
- **Workstream #7:** Update data security plans, breach readiness

WORKSTREAM #1: INFO GATHERING, SCOPING & HARMONIZATION

Info Gathering & Scoping

- Identify state(s) to which you are subject
- Identify practices subject to the respective laws
- Identify appropriate stakeholders
- Identify external resources (e.g., counsel, vendors)

Harmonization

- Identify existing privacy compliance program
- Conduct gap analysis against current practices
- Make risk-based decisions to incorporate new processing activities



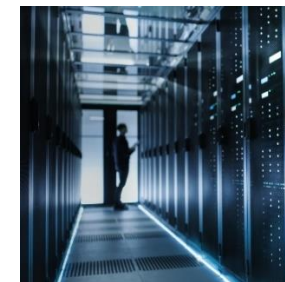
Privacy



Legal



Other Depts.



Tech Ops

WORKSTREAM #2: CREATE DATA INVENTORIES/MAPS

Complete a “data inventory” or “data mapping” exercise

Result of data mapping is a record that can be used to inform state compliance activities and risk-based scoping decisions

Optional, but helpful task

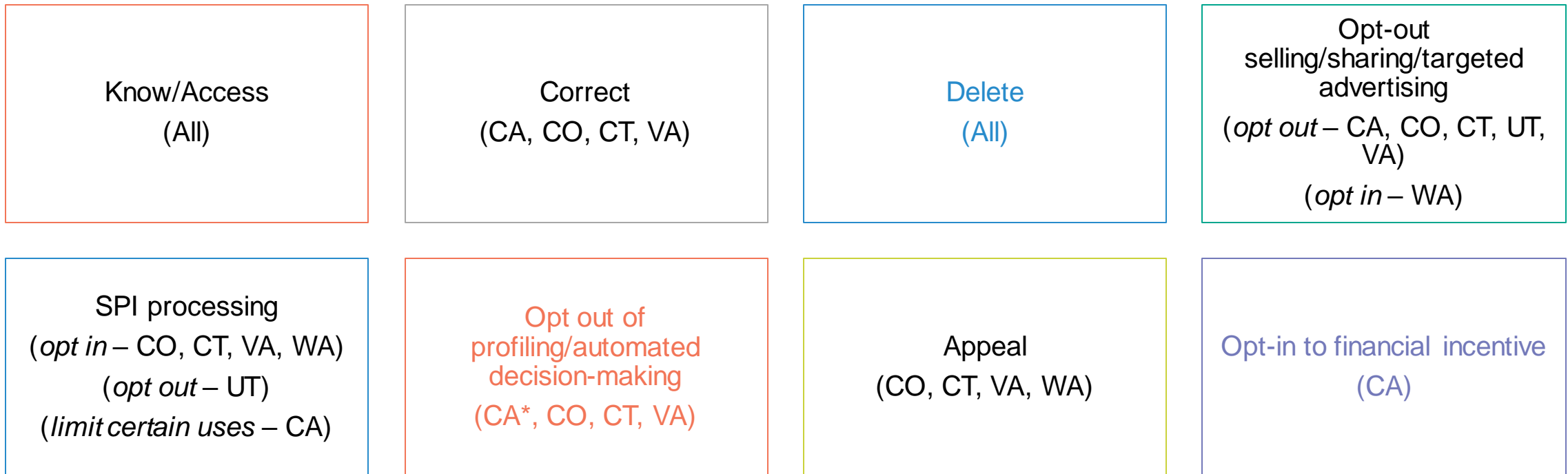
WORKSTREAM #3: UPDATE PRIVACY POLICY(IES)

Specific information is typically required in privacy policy

(e.g., types of personal information collected, uses of personal information, whom it is shared with, etc.)






Existing policies may need to be updated & should be updated annually

WORKSTREAM #4: REVIEW/UPDATE DSR PROCEDURES



Each state includes a right to **non-discrimination**

COLORADO CONSENT REQUIREMENTS

- **Consent** = affirmative, freely given, specific, informed and unambiguous
 - Clear, affirmative action  either deliberate and clear conduct or a clear statement of acceptance to processing terms (min. requirements to be informed, see below)
 - Freely given  may refuse consent without detriment and easily revoke at any time
 - Specific  names the specific different processing purposes, permitting separate consent by purpose
 - Informed  minimum standard of information to disclose to consumer, such as the controller identity, plain-language reasons for consent, processing categories & purposes
 - Unambiguous  consent obtained through use of dark patterns is not valid consent

PRIVILEGED / FOR EDUCATIONAL PURPOSES /
NOT TO BE USED AS LEGAL ADVICE

OPT OUT OF SALE / TARGETED ADVERTISING

- **Sale** (all states) – disclosing/making PI available to third parties for consideration (often includes exemptions for “service provider” and others)
- **Sharing** (CA) – disclosing/making PI available to third parties for targeted advertising regardless of consideration
- **Sharing** (WA) – disclosing consumer health data, except to a Processor
- **Targeted advertising** (CT, CO, UT, VA) – displaying ads based on inferences from PI collected over time and across unaffiliated websites/applications

WORKSTREAM #5: CREATE/UPDATE VENDOR/DATA RECIPIENT CONTRACTING PROGRAM

- Specific terms required in contracts with vendors that receive personal information
- Potential challenges depending on the type of vendor (e.g., adtech vendors)
- Update contracts with service providers/vendors with terms designed to protect personal information you share with them

WORKSTREAM #6: UPDATE GOVERNANCE, DOCUMENTATION & TRAINING

Internal policies

- Update and/or develop internal policies to support compliance (e.g., internal privacy policies, data retention policy, record keeping)

Training

- Develop & implement training materials

High-risk processing

- Determine whether the business engages in any “high-risk processing” (e.g., processing SPI, profiling)

WORKSTREAM #7: UPDATE DATA SECURITY PLANS, BREACH READINESS

Breach notices

- Privacy laws have security and breach notification requirements, are tied to breach notification laws

Security policies

- Review and update security policies to meet “reasonableness” standard

Update plans

- Update incident response plan, acceptable use policy, etc.

TAKEAWAYS

1. Think beyond the “legal requirements” and think consumer expectations
2. Devil is in the details; can you actually operationalize a state’s requirements (and operate there)
3. Education is paramount
4. More lead time is needed than you may think
5. A lot of options to implement – no “one size fits all.” Make a risk-prioritized plan because impossible to “do it all” (at least right away)
6. Test before launching

THANK YOU / QUESTIONS?

This material is for general information purposes only and should not be construed as legal advice or any other advice on any specific facts or circumstances. No one should act or refrain from acting based upon any information herein without seeking professional legal advice. McDermott Will & Emery* (McDermott) makes no warranties, representations, or claims of any kind concerning the content herein. McDermott and the contributing presenters or authors expressly disclaim all liability to any person in respect of the consequences of anything done or not done in reliance upon the use of contents included herein.

*For a complete list of McDermott entities visit mwe.com/legalnotices.

©2021 McDermott Will & Emery. All rights reserved. Any use of these materials including reproduction, modification, distribution or republication, without the prior written consent of McDermott is strictly prohibited. This may be considered attorney advertising. Prior results do not guarantee a similar outcome.

