Privacy Law Update:

New Trends and Compliance Requirements for 2024

June 13, 2024

Agenda

1. New State Consumer Privacy Laws
2. Amendments to Existing Law
3. The American Privacy Rights Act

New State Privacy Laws

2024: The Year of Data Privacy (Again)

Six states have passed privacy bills in 2024 (so far)

- One less than 2023

Thirteen new consumer privacy laws taking effect

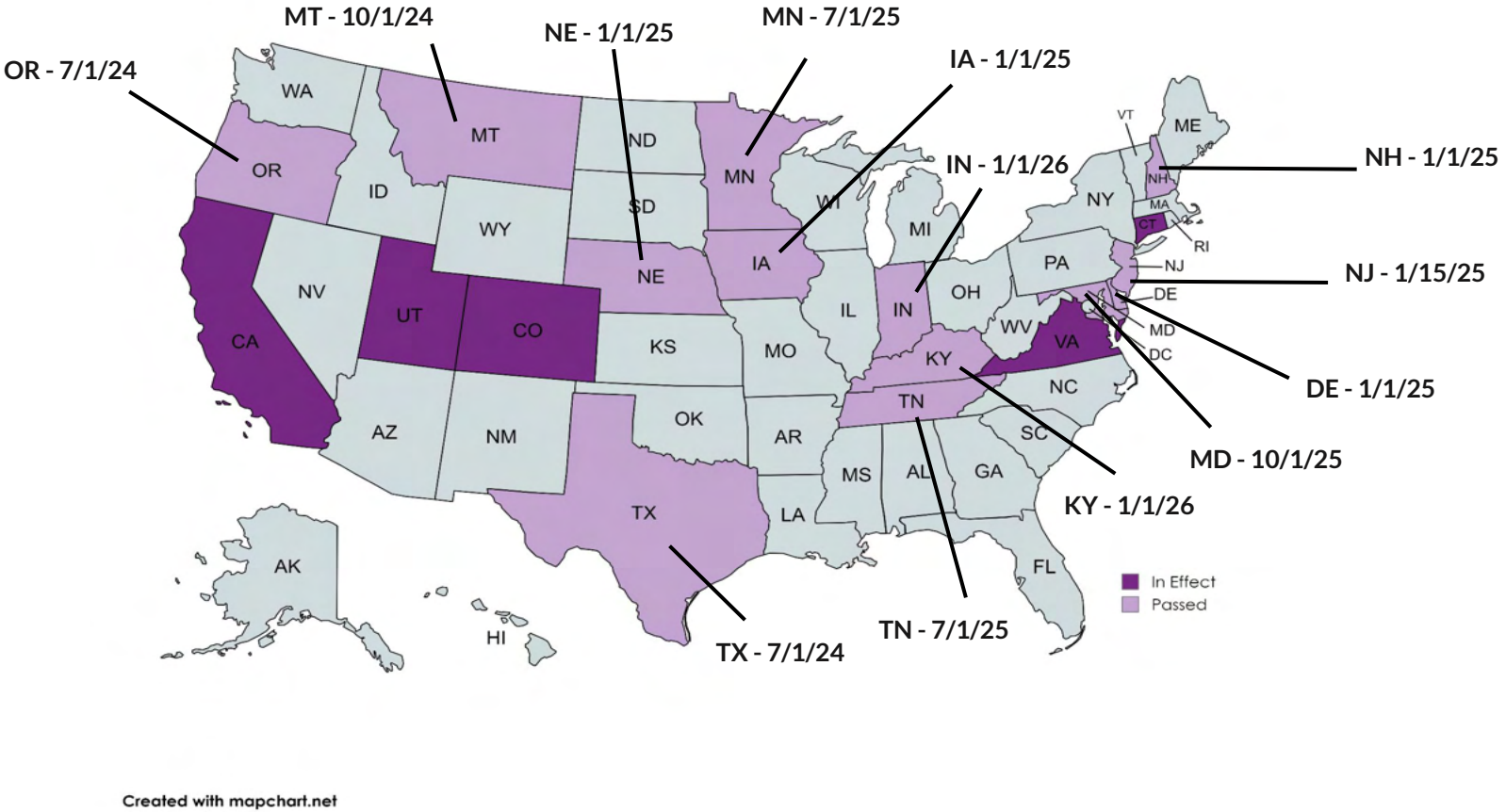
- Between July 1, 2024 and January 1, 2026

No sign of slowing down

- Ten more states considering privacy bills

They're all (relatively) similar

Privacy Law Tracker



For Today's Discussion:

- **Texas -** July 1, 2024
- **Oregon -** July 1, 2024
- **Montana -** October 1, 2024
- **New Hampshire -** January 1, 2025
- **Iowa -** January 1, 2025
- **Delaware -** January 1, 2025
- **Nebraska -** January 1, 2025
- **New Jersey -** January 15, 2025

Key Similarities

Required Documents

Privacy Notice

Data Processing Agreements

Data Protection Assessments (except IA)

Consumer Rights

Right to Know

Right to Correct

Right to Delete

Right to Port

Right to Opt-Out of Sales, Targeted Ads & Profiling

Right to Appeal

Enforcement

Overseen by State AGs

Penalties of $7,500 to $10,000 per violation

Attorney's Fees

Mandatory Cure Period

Regulatory Authority in NJ

No Individual Right to Sue (Yet)

Differences: Who Has to Comply?

Two states use novel applicability thresholds

- TX/NE - Businesses that collect/sell any Personal Data except for “Small Businesses” as defined by the federal Small Business Administration
    - Small businesses still have to comply with prohibition on selling Sensitive Data without consent

Three others use significantly lower thresholds

- MT - Data from 50K+ residents (or 25K plus 25% of revenue from data sales)
- DE - Data from 35K+ residents (or 10K plus 20% of revenue from data sales)
- NH - Data from 35K+ residents (or 10K plus 25% of revenue from data sales)

Differences: Right to Know Disclosures

Oregon gives consumers a new way to exercise the Right to Know

- Obtain a "list of specific third parties" that a business has disclosed their data to
  - Businesses have the option to instead provide a list of the third parties they have disclosed any data to
- First state to require this level of specificity

Differences: Children's Data

Several states add protections for children between 13 and 18

- Most existing states use federal COPPA definition of "child" (under 13) and don't impose many protections for teens
- DE, NJ, NH, OR, and MT now restrict businesses from selling data from teens or using it for targeted ads without first getting consent

Similar protections in CO and VA starting in 2025

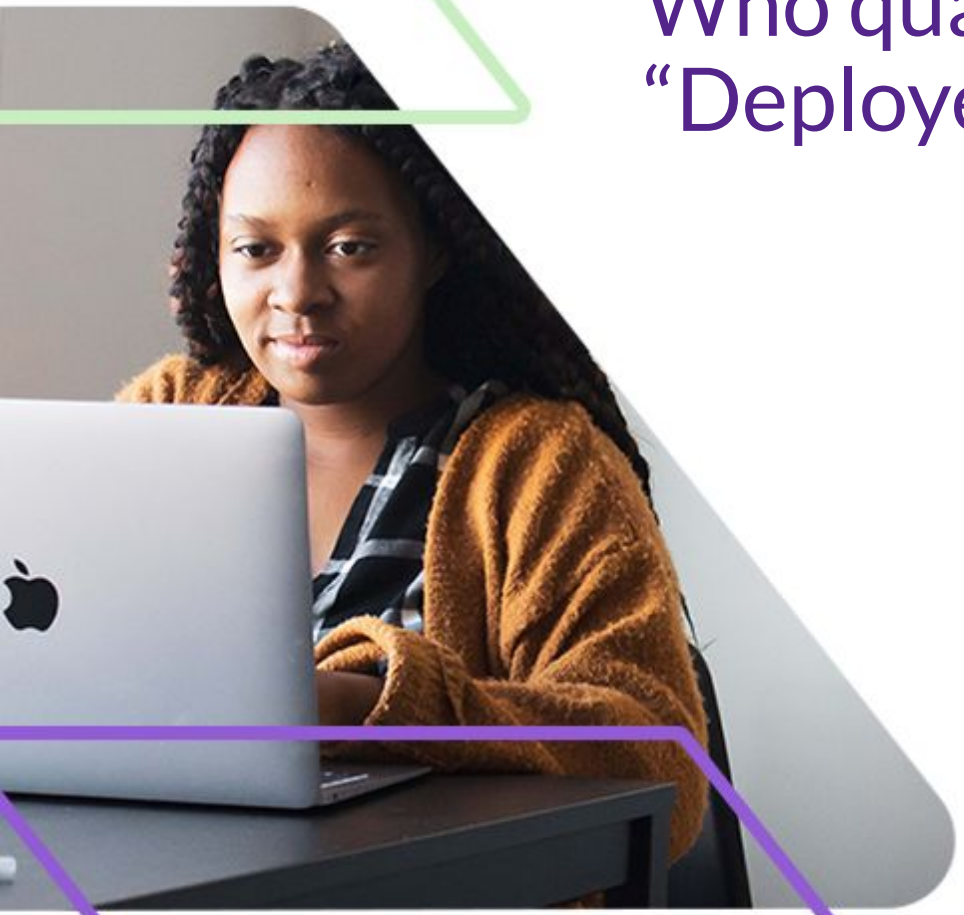
- Restrictions on selling/targeted advertising/profiling children's data without consent, but age remains 13

"Known or should have known" standard remains and is consistent across states

- Generally only a risk if a business actually knows its customers are children or the business' products/services are geared toward children

Colorado's Artificial Intelligence Act

- First **comprehensive regulation of AI** at the state level
- Regulates both "Developers" and "Deployers" of AI systems
- No private right of action
    - Will be enforced exclusively by the Colorado Attorney General's Office
- Takes effect February 1, 2026



Who qualifies as a “Deployer” of AI?

A “deployer” is a person doing business in Colorado that uses an AI system to help make decisions that have a substantial effect on:

- Employment or employment opportunity
- Education enrollment or opportunity
- Financial or lending services
- Essential government services
- Healthcare services
- Housing
- Insurance
- Legal services

Deployer Responsibilities

Deployers of AI have an obligation to use "reasonable care" to prevent "algorithmic discrimination."

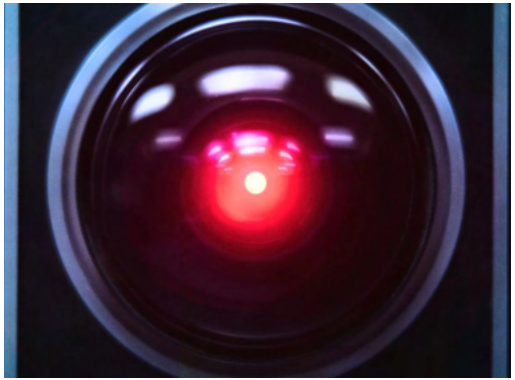
There is a rebuttable presumption that deployers used reasonable care if they take certain steps, including

- Implementing a risk management policy and program for high-risk AI systems
- Completing an impact assessment of high-risk AI systems
- Notifying consumers that could be affected by decisions made by high-risk AI systems
- Making a publicly available statement summarizing the types of high-risk systems that the deployer currently deploys
- Disclosing to the attorney general the discovery of algorithmic discrimination within 90 days of discovery

Amendments to Existing Law

Colorado: Adds Protections for Biologic and Neural Data

- Colorado expanded the definition of “sensitive data” to include biologic and neural data.
- Biologic data includes genetic, biochemical, physiological or neural properties, compositions or activities, and includes neural data.”
- Neural data is defined as “information that is generated by the measurement of the activity of an individual’s central or peripheral nervous systems and that can be processed by or with the assistance of a device."
- The effective date for the new law is August 6, 2024.



Colorado: Protection for Biometric Identifiers

A wider scope

- The CPA generally applies only to organizations that meet certain thresholds.
- The new protections apply to individuals or organizations that control or process **one** or more biometric identifiers.
- Applies to the data from employees and contractors as well as consumers.

Biometric Identifiers

- The law provides some helpful examples of biometric identifiers:
  - A fingerprint
  - A voiceprint
  - A scan or record of an eye retina or iris
  - A facial map, facial geometry, or facial template

Requirements / Limitations

- Written policy that includes:
  - A retention schedule for biologic identifiers
  - A protocol for responding to data security incidents
- Affirmative consent before biometric identifiers are collected
  - Consent can be required of employees for time keeping and workplace security purposes

* Effective date July 1, 2025

CCPA Regulations - Round 2

CPPA began Preliminary Rulemaking Process in December 2023

- Updated draft released in March

Rules for Risk Assessments and "Automated Decisionmaking Technology"

- Includes, but is not limited to AI

Formal Rulemaking expected to begin this fall

- Still a long way to go

Risk Assessments in California

Mandatory any time a Business:

- (1) Sells data, (2) engages in targeted advertising, (3) processes sensitive data, (4) conducts "Automated Decisionmaking," or (5) trains AI

All "Relevant Individuals" must contribute

- Employees whose " job duties pertain to the processing activity"

Must submit Assessments to the CPPA annually

- Unless the processing activity was not initiated

Automated Decision-Making Technology

Expansion of existing laws' treatment of "Profiling"

- Regulates any use of automated technology in making decisions that substantially affects people

Would require businesses to:

- (1) present consumers with ADT-specific notices, (2) conduct Risk Assessments, (3) allow consumers to opt-out, and (4) provide information about their use of ADT upon request

Expansive right to access information related to specific use of ADT

- Businesses will have to provide individualized explanation of how the ADT process made a specific decision

Prospects for a Federal Privacy Law

A Brief History of Federal Privacy

US takes a “sectoral” approach to privacy at the federal level

- HIPAA, FERPA, GLBA, etc.

Comprehensive laws have failed to gain traction

- Some believe sectoral approach is more effective
- Opposition from big businesses (especially Big Tech)

Last attempt was the American Data Privacy Protection Act (2022)

- Failed due to disagreements around preemption of state law and private right to sue (mostly)

The American Privacy Rights Act

A BILL

To [_____], and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "American Privacy Rights Act of 2024".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Introduced in the House in April

- Sponsored by Sen. Maria Cantwell (D) and Rep. Cathy Rogers (R)

Combines the ADPPA with other proposals

- More bipartisan buy-in than previous attempts

Currently under consideration in the House Committee on Energy and Commerce

- Long way to go, but early signs are encouraging
- Significant amendments already, with more to come

The American Privacy Rights Act

Substantively similar to state consumer privacy laws

- Core consumer rights and business obligations are identical to existing laws

Would apply to all businesses that control data and:

- Have an annual gross revenue >$40 million/year;
- Collect, process, retain, or transfer data from more than 200,000 people*; **OR**
- Sell any amount of data

Other notable provisions:

- Preempts all state consumer privacy laws (with exceptions)
- Allows individuals to sue businesses for violations
- Requires consent for all transfers of sensitive data to third parties

Q&A time!

Book a no-pressure demo of SixFifty Privacy