Privacy Law Update: New Trends for 2025

December 12, 2024

Agenda

1. New state consumer privacy laws
2. Changes to existing law
3. AI & biometrics: the next privacy frontier

New state privacy laws

2024: Building momentum

Seven states have passed privacy bills in 2024

- The same as 2023

Three new state laws took effect in 2024

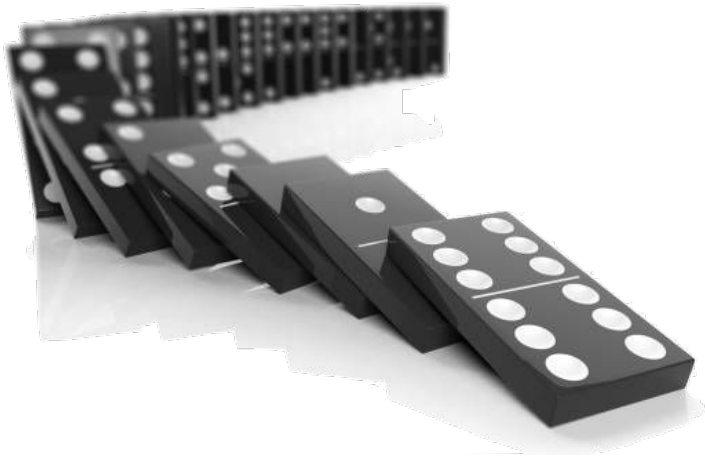
- Montana, Oregon, and Texas

No sign of slowing down

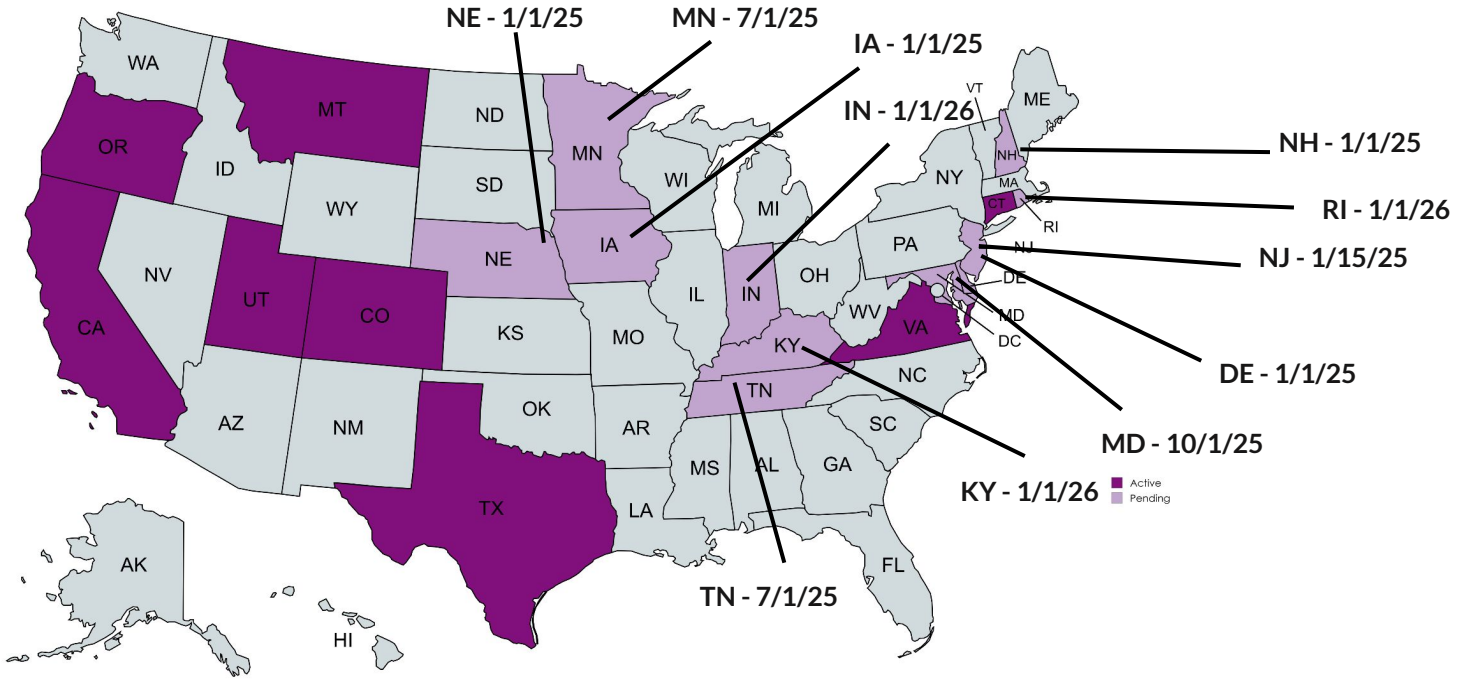
- Three more states with active privacy bills (MI, OH, and three in PA)
- Fourteen other states and 37 other bills proposed

Eleven new consumer privacy laws taking effect

- Between January 1, 2025 and January 1, 2026
- Five effective in January, 2025



Privacy law tracker



Created with mapchart.net

SIXfifty

For today's discussion:

- **Delaware**
  - January 1, 2025
- **Iowa**
  - January 1, 2025
- **Nebraska**
  - January 1, 2025
- **New Hampshire**
  - January 1, 2025
- **New Jersey**
  - January 15, 2025

Common ground

Required Documents

- Privacy Notice
- Data Processing Agreements
- Data Protection Assessments (except IA)

Consumer Rights

- Right to Access
- Right to Correct (except IA)
- Right to Delete
- Right to Port
- Right to Opt-Out of Sales, Targeted Ads and Profiling (except IA)
- Right to Appeal

Enforcement

- Overseen by State AGs
- Penalties of $7,500 to $10,000 per violation
- Attorney's Fees
- Mandatory Cure Period
- No Individual Right to Sue
    - Proposed law in VT vetoed

SIXfifty

Differences: Applicability

Novel applicability threshold

- 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

Two use significantly lower thresholds

- 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)

Two use significantly higher thresholds

- IA - Data from 100K+ residents (or 25K plus 50% of revenue from data sales)
- NJ - Data from 100K+ residents (or 25K plus any revenue from data sales)

SIXfifty

Differences: Consumer-friendly laws

Delaware, Nebraska, New Hampshire, New Jersey

- Broad applicability, particularly in:
    - Nebraska (applies to all businesses that process or sell personal data unless they are a “small business”); and
    - New Jersey (no revenue threshold for data sales; just sale of 25K+ consumers)
- Provide all existing consumer rights
- Impose all existing business obligations
- 30 to 60-day cure periods
    - 3 of those periods set to expire
- Provision for additional future regulations (NJ)

Differences: Business-friendly laws

Iowa doesn't seem to want to punish businesses

- High applicability threshold
- Fewer ways to violate the law
- Up to $7,500 penalty per violation
- 90 days to cure any violation of the law
    - Longest cure period in the nation
    - No sunset date

SIXfifty

Changes to state law

New regulations in the new year

Two sets of new CCPA regulations in 2025:

- One clarifying who has to register as a "data broker"
  - Likely to kick in January 1, 2025
- **One creating rules for Cybersecurity Audits, risk assessments; and Automated Decision-Making Technology ("ADMT")**
  - Open for public comment through January 14, 2025
  - Final vote likely to follow in March or April
  - Will take effect sometime around Spring or Summer 2025

sixfifty

The CPPA wants you to be a data broker

Data Brokers are businesses that sell data about consumers that they don't have a "direct relationship" with

- Under the new law, selling *any* data that wasn't obtained directly from the consumer will qualify
  - Even if the business has a relationship with and gets other data from that consumer

Qualifying businesses must register before January 31 by:

- Paying a $400 registration fee; and
- Providing detailed information about the business' data practices to the CPPA

Data Brokers are subject to more scrutiny than most businesses, and it's likely they will face more regulation from the CPPA over time

sixfifty

Good things (and regulations) come in threes

Cybersecurity Audits

Required for businesses that:

- Process lots of data, or
- Make most of their revenue from selling/sharing

Audits must:

- Document the establishment, implementation, and maintenance of the business' cybersecurity program; and
- Address 18 specific aspects of the program, listed in the regulations.

Businesses must certify their compliance to the CPPA annually

Risk Assessments

Required each time a Business:

- Sells or "Shares" data;
- Processes sensitive data;
- Uses ADMT; or
- Trains AI on CA data

Assessments must compare:

- Risks to consumer privacy; against
- Benefits to business and other stakeholders

Must submit Assessments to CPPA annually

ADMT

Limits when and how businesses use ADMT to make "significant decisions"

- "ADMT" is defined broadly
- Includes predictive algorithms, AI, and more

Would require businesses to:

1. Add ADMT-specific info to their privacy notices
2. Conduct Risk Assessments,
3. Allow consumers to opt-out, and
4. Provide information about how ADMT was used to make a decision about a specific consumer upon request

sixfifty

Opt-Out Preference Signals

Connecticut, Texas, and Montana to require businesses to recognize Opt-Out Preference Signals starting January 1, 2025

- Businesses that sell data, share it for targeted advertising, or use it for profiling are covered

Signals are sent by a consumer's web browser or device to communicate their desire to opt out

- Can be used to opt out of sales, targeted advertising, and/or (sometimes) profiling

Implementation is a technical question, so check with your technical team or website host

- The Global Privacy Control provides a guide here

sixfifty

The status of enforcement

Enforcement has been slow, but is set to pick up in 2025

- Mandatory cure periods will lapse in some states; and
- Enforcement infrastructure grows in others

To date, enforcement has focused on:

- Disclosures around selling/sharing data;
  - Sephora - $1.2 million
- Failure to properly process consumer requests; and
  - Doordash - $375,000
- Improper use of sensitive data
  - Tilting Point Media - $500,000

Use of AI and biometric data likely targets for future efforts

- Texas v. Meta - $1.4 billion

sixfifty

AI & Biometric Data

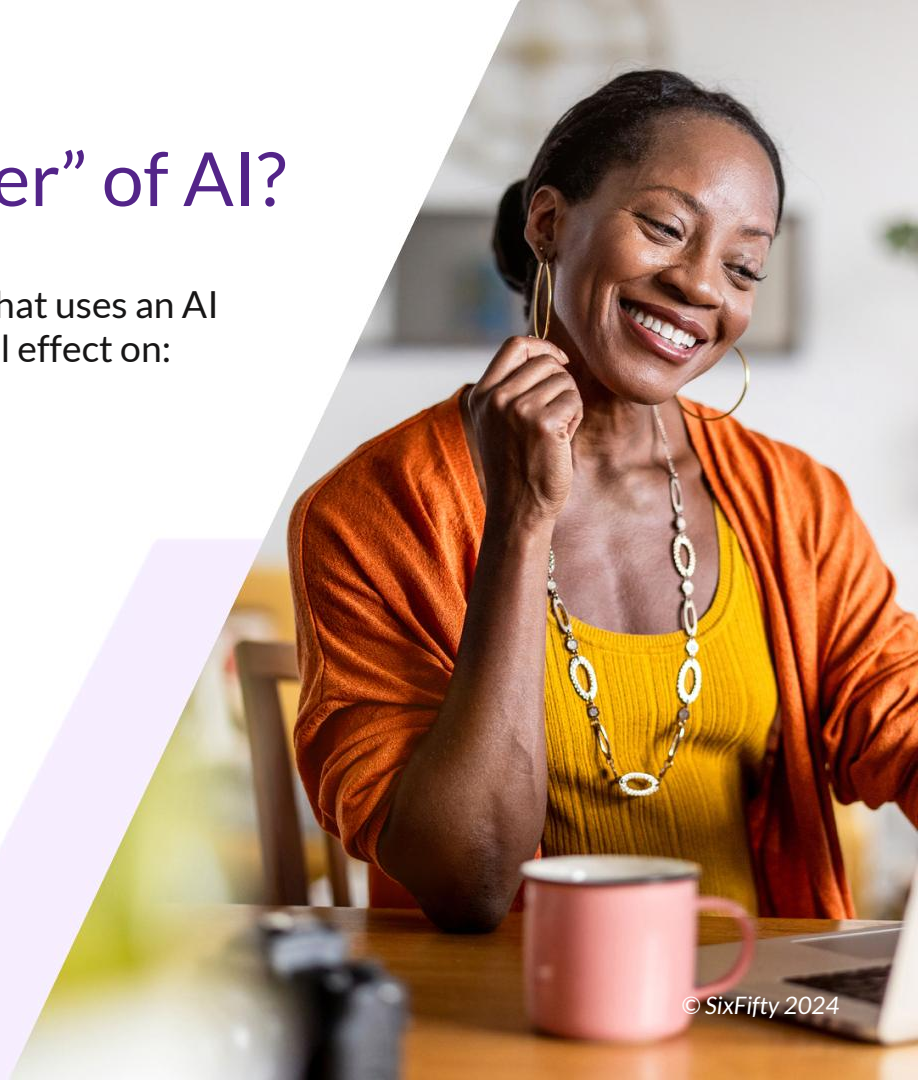
Colorado's Artificial Intelligence Act

- Enacted on May 17, 2024
- 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 who 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

sixfifty

Illinois's new AI law

- Enacted on August 9, 2024, and takes effect January 1, 2026
- Not as comprehensive as Colorado's AI Act
- Similar in scope but less onerous than NYC Local Law 144
- Bars employers from using AI if it discriminates against protected classes or uses zip codes as a proxy for protected classes
- Requires employers to notify employees when they use AI to make employment decisions
- Enforced by the Illinois Department of Human Rights and Illinois Human Rights Commission

Colorado's protection 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 new provisions took effect on August 6, 2024.

sixfifty

Colorado's protections 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

sixfifty

Thank you!

Schedule a no-pressure
1:1 tour of SixFifty

Learn more at sixfifty.com