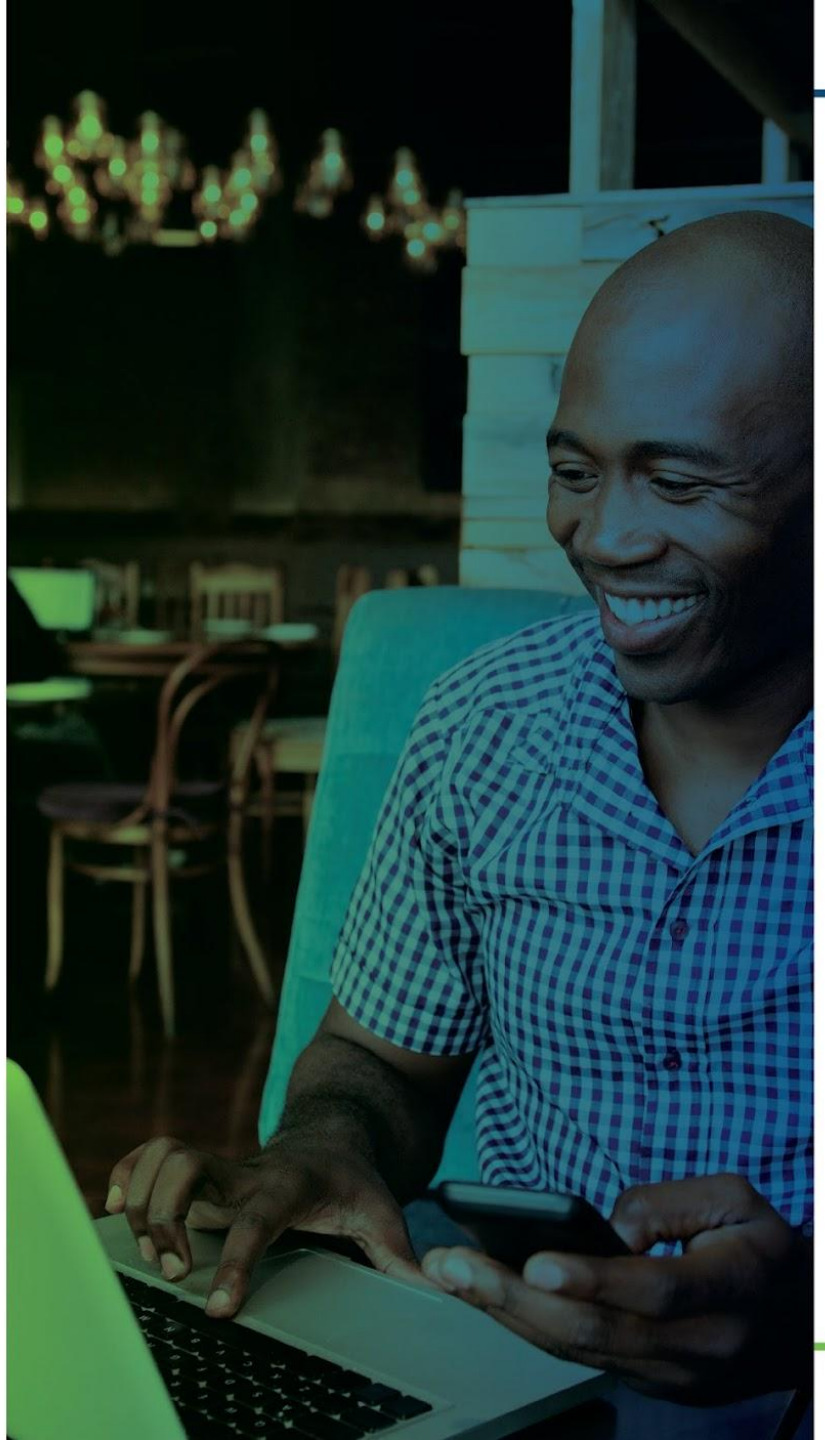


Regulation Radar: A Guide to Today's US Data Privacy Laws

Tuesday, 23/January/2024

8:00-9:00 PST
11:00-12:00 EST
17:00-18:00 CEST

Welcome and Introductions

Panelists

Sheri Porath Rockwell
CIPP/US,CIPP/E
Counsel
Sidley Austin LLP

Andy Blair
CPO
Universal Music Group

David Ray
CIPP/US, CIPM, CIPT
CPO
BigID

Agenda

1. Overview of US State Privacy Laws
2. New Laws by Right / Responsibility
3. Sectoral & Unique Aspects
4. Federal Actions and Private Litigation
5. Operational Challenges
6. What's next? Privacy Predictions for 2024

Where do we stand in 2024

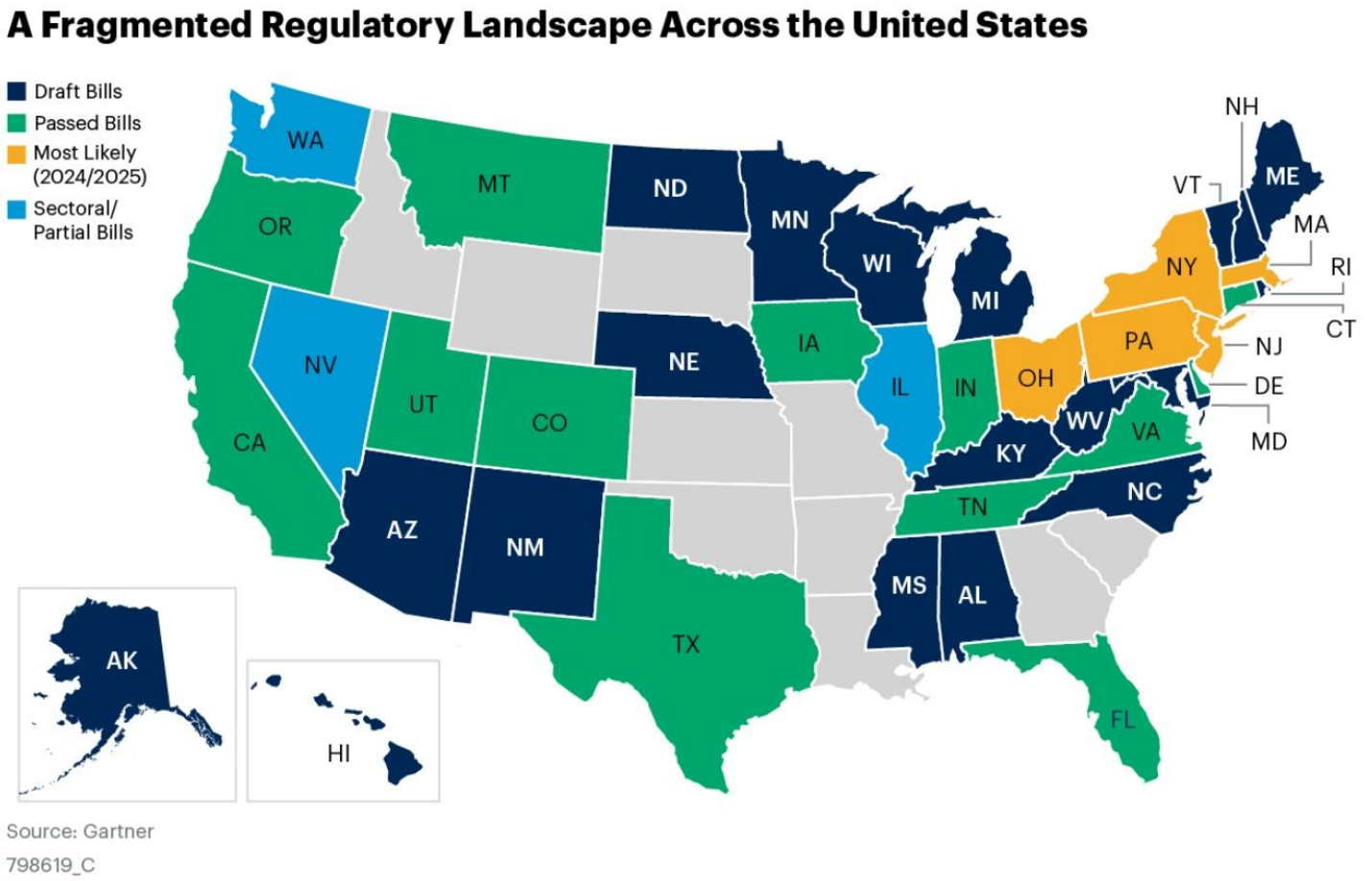
Effective Dates

2023
California, Colorado, Connecticut, Utah, and Virginia.

2024
Florida, Montana, Nevada, Oregon, Texas, Washington.

2025
Delaware, Iowa, New Jersey, Tennessee.

2026
Indiana.



Proposals & Predictions

2024 predictions based on the past year
Kentucky, Maine, Massachusetts, Missouri, New York, Ohio, Pennsylvania, Vermont, West Virginia, and Wisconsin.

NJ SB 332 was enacted on Jan. 16, 2024.

NH SB 255 passed by the legislature on Jan. 18, 2024.

Consumer Data Rights

What have we seen up to now?

- Most state privacy laws provide the following rights:
  - Access, Know, Confirm (or Combination of Access + Know or Confirm);
  - Delete;
  - Correct;
  - Portable Data;
  - Opt out of certain processing activities (details on Consent slide)

What's new?

- Several of the state privacy laws taking effect in 2024, and beyond, have incorporated some unique twists to the rights granted to individuals.
  - DPDPA: Delaware consumers have the right to obtain a list of categories of third parties to whom their personal data was disclosed.
  - OCPA: Oregon consumers can request a list of third parties to whom their personal data was disclosed.
  - INCDPA: Indiana grants controllers discretion over whether to provide consumers a standard report or a representative summary of their personal data when responding to an access request.
  - TDPSA: Texas imposes limited restrictions on for-profit entities that are classified as "Small Businesses" by the US Small Business Administration (SBA).

What's the impact on covered organizations?

- Covered organizations will need to determine how to account for the increasing number of state laws and the different requirements set forth in each of them for compliance purposes.

Consumer Opt-Out Rights

What have we seen up to now?

- Most state privacy laws provide opt out rights when processing personal data for the purposes of:
  - Targeted advertising;
  - The sale, and more recently, share of personal information; and
  - Profiling that results in legal or similarly significant harm.
- Some state privacy laws also require businesses to obtain consent from a consumer prior to processing sensitive data, or in the case of California, limit the use and disclosure of sensitive personal information.

What's new?

- Many state privacy laws taking effect in 2024, and beyond, have incorporated provisions concerning automated decision-making and artificial intelligence; specifically, granting opt out rights when conditions apply.
  - California and Delaware prohibit businesses from making decisions about an individual based solely on automated processing, without human input, whereas Utah does not recognize the right.
  - The remaining states provide the right to opt out of automated decision-making when explicit circumstances arise.

What's the impact on covered organizations?

- How are organizations implementing these rights?
- Do you give all rights to individuals across states, or do you only allow these rights for the specific states?

Universal Opt-Out Mechanisms (UOOMs)

What have we seen up to now?

- California and Colorado were the first to require businesses to implement a universal opt out mechanism (UOOM), such as the Global Privacy Control (GPC), that allows an individual to voluntarily provide or revoke consent before the organization processes the individual's personal information.

What's new?

- Several more states have chosen to require recognition of UOOMs, including CT, DE, MT, NJ, and OR.
- While a finalized version of the Act has not yet been posted, the current text of the newly enacted NJ SB 332 provides a wrinkle for UOOMs that enables a consumer to opt out for profiling. The language was struck in Section 8(b)(1) of the bill, however, the language remains in Section 8(a) predicated on the condition, *"...When such technology exists."*
- Partially, Required: TX; only required if the controller is obligated to recognize such signals pursuant to the law of another state.

What's the impact on covered organizations?

- Websites need to include technology solutions that support recognized UOOMs.
- A key challenge is where states like CA require that the UOOM preference be saved and follow a "known" user.

Data Protection Assessment (DPA)

What have we seen up to now?

- Until recently, DPAs have not been required in the US, as they are in Europe.

What's new?

- With the exception of Iowa and Utah, most of the latest state privacy laws require that businesses conduct a DPA when engaged in certain processing activities, including when selling personal data, using personal data for targeted advertising or profiling purposes, and processing sensitive data. Below are some notable variations:
  - The California Privacy Protection Agency (CPPA) has released draft proposals for AI, cybersecurity, and risk assessments. Accordingly, California does not yet mandate DPAs.
  - In addition to the DPA provisions provided by many of the other state laws, Colorado has a few extensive requirements.
  - Oregon and Colorado provide DPA retention periods of five and three years, respectively.

What's the impact on covered organizations?

- Ideally, state DPAs could be combined with existing GDPR DPIA processes, though variations in triggers and requirements will create challenges.
- Learning curve for US-focused organizations doing these for the first time.

Record-keeping Requirements

What have we seen up to now?

- California was the first state to permit businesses to preserve a confidential record of deletion requests for "the purposes of preventing the personal information of a consumer who has submitted a deletion request from being sold" and for compliance with the law or other purposes permissible under the CCPA.

What's new?

- Businesses must preserve records of deletion requests and maintain the minimum volume of data necessary to ensure the individual's personal information is deleted, as is required by most comprehensive state privacy laws, with the exception of Iowa and Utah.
- California and Colorado require businesses to retain records of rights requests for 24 months. These laws also set forth specific requirements concerning the contents of such records (e.g., date, nature of the request, business response, and so forth).
- Businesses covered by California privacy laws must track certain metrics on an annual basis, relating to consumer requests received, such as whether a request was processed or denied in whole or in part.

What's the impact on covered organizations?

- Potentially technically challenging for many organizations given the complexity of typical consumer marketing tech stack.
- Software and systems that are used to manage data subject rights, consent, and even cookie management must provide enough detail to support record-keeping requirements

Know Your Vendors

What have we seen up to now?

Subject to certain provisional changes and/or exemptions, all 13 (soon 14) state comprehensive privacy laws require controllers and processors to enter into contracts that set forth processing instructions as well as other contractual obligations, such as:

- The nature and purpose for processing personal information, along with the type of personal information being processed and the duration of the processing;
- The rights and obligations of both parties, including a requirement that processors engage subprocessors pursuant to a contract that has the same or similar processing obligations;
- The processor must agree to permit and cooperate with reasonable assessments, audits, or inspections carried out by a controller; and
- To return or delete any processed personal data to the controller once the provision of Services or the parties' Agreement expires.

- Unlike the other states, California requires separate contracts that contain explicit and varying provisions for 'Service Providers', 'Contractors', and 'Third Parties', as those terms are defined by the CCPA.
  - Contracts for Service Providers and Contractors primarily contain the same provisions, with a few additional requirements for Contactors. Notably, the CCPA states that if a business contracts with these types of processors to provide cross-context behavioral advertising (CCBA), then the processor will be deemed a third party.
  - Third parties—potentially, as a mechanism to prevent businesses from employing them—are not permitted to collect, use, process, retain, sell, or share PI made available by a business if it does not have a contract that complies with the CCPA.

What's new?

- State consumer privacy laws are not the only reason businesses should know who is posting content on their websites. Newly, enacted state consumer health data laws contain prohibitions on geotracking, meaning that covered businesses could be in violation of such laws if consumers' locations are revealed through tracking technologies.
- Similarly, the FTC has already issued two proposed orders (X-data/Outlogic, InMarket) this year aimed at limiting the collection, use, and sale of consumers' location data. A third complaint was filed by EPIC against Google last week, requesting the FTC investigate for "unfair and deceptive practices" concerning how it handles data; specifically, that Google violated its promise to delete sensitive user location information.

What's the impact on covered organizations?

- Privacy teams should regularly monitor and review any new trackers found; identify the category of the tracking technology (e.g., third-party cookie, web beacon, scripts, etc.); and determine whether it is permitted based on legal and contractual obligations.
- Businesses that employ cookies to collect, process, sell, or share personal information should review state comprehensive privacy laws since these laws typically address activities and/or requirements that may apply to cookies and similar tracking technologies, such as: (1) Targeted advertising; (2) Sale and sharing of personal data; (3) Profiling; and (4) User tracking.
  - For instance, CTDPA-covered businesses that receive consumer requests to opt out of targeted advertising must cease transmitting the consumer's personal information to third parties. Otherwise, the activity may be considered a sale under the CTDPA.

Outliers and Sectoral State Laws

- **Online Platforms/Sales of SPI:** The Florida Digital Bill of Rights restricts government institutions from engaging in certain activities involving social media platforms, and mandates online platform services implement controls to protect children's personal and sensitive data. Most of the remaining provisions of the law only apply to businesses whose annual revenue is $1B or more; however, persons doing business in the state and that sell sensitive personal data are subject to opt-in consent requirements for such sales and website labeling requirements.

- **Consumer Health Data:** The Washington 'My Health My Data' Act and the Nevada Consumer Health Data Act (SB 370) apply to businesses that collect, process, or transfer consumer health data of state residents or associated with the state.
  - Requirements for opt-in consent to process consumer health data
  - Access controls
  - Consumer health data policies
  - Right to know all third party data recipients
  - Geofencing

  Connecticut expands its privacy law to apply to all controllers that process consumer health data and treat consumer health data as "sensitive" personal data requiring opt-in consent.

- **California DELETE Act:** Expanded registration requirements and 2026 data opt-out tool with auditing

A handful of states also passed laws in 2023, concerning:

- The data privacy of children or minors (e.g., the California Age Appropriate Design Code Act);
  - Colorado proposed a bill (SB24-041) concerning data protections for a minor's online activity.
  - South Carolina introduced its own version (HB 4842) of an Age Appropriate Design Code Act.
- Social media companies and requirements for parental control;
- Age verification of minors for websites containing adult content; and

Federal Actions and Private Litigation

- **US Privacy Law -** Status / predictions
- **FTC Enforcement Actions**
  - 2023 Year of Health Data:
  - 2024 Year of Location Data (?)
  - ANPRM Status
  - COPPA 2.0
- **Other Agencies**
  - FCC
  - CFPB
  - HHS
- **Private Litigation**
  - Pen Register
  - Chatbot/Session Replay
  - VPPA

How Are Companies Operationalizing?

- Organizational buy-in and risk appetite.
  - Companies have different priorities and motivators.
  - Figure out what works and make friends.
  - Ahead of the curve or hang on as long as you can?
- Managing inconsistencies.
  - Many companies adopt a harmonized approach across states/countries.
  - Build for long-term. This isn't going away!
- Minding the cross-functional issues.
  - Consider impacts AI, security, governance, audits, and more.

Most importantly, start!

What's Next? 2024 Privacy Predictions

- US state privacy laws will continue to proliferate in the absence of comprehensive federal privacy legislation, and AI will be a focus area
- Similar to its role in privacy, California will take the lead in AI legislation
- There will be a greater emphasis on protections for biometric, genetic, and related forms of consumer health data.
    - Colorado recently proposed a bill (HB 24-1058) that would expand the CPA's definition of sensitive data to include "biological data" and "neural data".
    - Vermont introduced a comprehensive privacy law that contains requirements for biometric data.
- Expect more states to pass laws regulating data brokers. Currently, only California, Vermont, Oregon, and Texas have enacted such laws.

Questions and Answers

Panelists

Sherry Rockwell
CIPP/US,CIPP/E
Counsel
Sidley Austin LLP

Andy Blair
CPO
Universal Music Group

David Ray
CIPP/US, CIPM, CIPT
CPO
BigID

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: IAPP TO ADD SURVEY LINK HERE

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation please
contact:

livewebconteam@iapp.org