California Privacy Rights Act and U.S. Privacy Law Updates

Scott C. Hall
Partner

Mari S. Clifford
Associate

Sabrina A. Larson
Partner

Amber Leong
Associate

Bina Patel
Associate

Coblentz Patch Duffy & Bass LLP

Presentation Roadmap

- CPRA Overview
- Other U.S. State Law Developments
- Privacy Litigation Trends
- Data Breach Preparation and Response
- Key Action Items For Businesses

California Privacy Rights Act (CPRA)

1/1/2020	CCPA compliance deadline.
8/14/2020	California OAL approves Final Regulations.
11/3/2020	Prop 24 (CPRA) approved by California voters.
12/16/2020	CPRA takes effect but most provisions not operative until 2023.
1/1/2022	“Look back” period: CPRA’s right to know or right of access applies to personal information collected after this date.
7/1/2022	CPRA deadline for adopting final regulations.
1/1/2023	CPRA in full effect. B2B and employee exemptions expire.
7/1/2023	Enforcement of CPRA to begin.

California Privacy Rights Act (CPRA)

1/1/2020	CCPA compliance deadline.
8/14/2020	California OAL approves Final Regulations.
11/3/2020	Prop 24 (CPRA) approved by California voters.
12/16/2020	CPRA takes effect but most provisions not operative until 2023.
1/1/2022	"Look back" period: CPRA's right to know or right of access applies to personal information collected after this date.
7/1/2022	CPRA deadline for adopting final regulations.
1/1/2023	CPRA in full effect. B2B and employee exemptions expire.
7/1/2023	Enforcement of CPRA to begin.

CCPA and CPRA: How are they related?

CPRA is an amendment of the California Consumer Privacy Act (CCPA). It expands on several areas of the existing CCPA.

The California Office of the Attorney General will retain civil enforcement authority over the CCPA and CPRA.

Businesses who have thus far avoided or ignored CCPA obligations should immediately get in compliance for a few reasons:

It is the law in California and will be enforced by AG and new Privacy Protection Agency ("CPPA").

The CCPA contains a private right of action—and plaintiff's lawyers are already actively filing suit.

Applicability of the CPRA

- The CPRA maintained most of the CCPA definitions with a few notable exceptions.
- CPRA narrowed the definition of "businesses" covered by the privacy act and introduced new concepts of "sharing" information as liable as well.
- "Business"
  - A sole proprietorship, partnership, limited liability company, corporation, or other legal entities organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that meets one of the three thresholds described below;

Applicability (cont.)

- As of January 1 of the calendar year, had a granular gross revenue in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year.
- Alone or in combination, annually collects, buys, sells, or shares for cross-context behavioral advertising the personal information of 100,000 or more consumers or households, or
- Derives 50 percent or more of its annual revenues from selling or sharing behavioral advertising consumers' personal information.

*Only one of the three must be met for the CPRA to apply.

Applicability (cont.)

The CPRA maintains the CCPA's categories of personal information (PI) but adds the new subcategory of "sensitive personal information."

Personal Information

1. Identifiers
2. Characteristics of protected classifications
3. Commercial information
4. Biometric information.
5. Internet or other electronic network activity information
6. Geolocation data.
7. Audio, electronic, visual, thermal, olfactory, or similar information.
8. Professional or employment-related information.
9. Education information
10. Inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Applicability (cont.)

Sensitive Personal Information

1. Social security, driver's license, state identification card, or passport number;
2. Account log-In, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
3. Precise geolocation;
4. Information regarding a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
5. The contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;
6. Genetic data;
7. The processing of biometric information for the purpose of uniquely identifying a consumer;
8. Personal information collected and analyzed concerning a consumer's health; or
9. Personal information collected and analyzed concerning a consumer's sex life or sexual orientation

Selling Personal Information

What is "selling" information under the CCPA?

1. "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party *for* monetary or other **valuable consideration**.
2. Any disclosure of data for valuable consideration.
3. Cloud storage providers, HR/payroll services, advertising, email service providers?

Sharing Personal Information

The CPRA also introduced limitation on "sharing" personal information.

"Sharing"

- Refers to a business's disclosure of personal information to a third party for "cross-context behavioral advertising," regardless of whether the disclosure is also a "sale."
- "**Cross-context behavioral advertising**" is defined as the "targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."

In essence, this definition intends to capture the collection of a consumer's personal information across third-party digital properties for the purposes of *targeted advertising*.

- Under the CPRA, consumers have a separate right to opt-out of "sharing" personal information.
- A business must advise consumers of this new right through a clear and conspicuous link on the business's homepage titled "Do Not Sell or Share My Personal Information." This link replaces the current "Do Not Sell My Personal Information" link required by the CCPA.

Consumer Rights Under the CPRA (Modified CCPA Rights)

Right to Delete	Businesses are now required to notify third parties to delete any consumer PI bought or received, subject to some exceptions.
Right to Know	The PI that must be reflected in a "Right to Know" response is expanded to include PI collected beyond the prior 12 months, if collected after January 1, 2022.
Right to Opt Out	The opt-out right now covers "sharing" of PI for cross-context behavioral advertising as outlined below.
Opt in Rights for Minors	Extends the opt-in right to explicitly include the sharing of PI for behavioral advertising purposes. As with the opt-out right, businesses must wait 12 months before asking a minor for consent to sell or share his or her PI after the minor has declined to provide it.
Right to Data Portability	Consumers may request that the business transmit specific pieces of PI to another entity, to the extent it is technically feasible for the business to provide the PI in a structured, commonly used and machine-readable format.

Consumer Rights Under the CPRA (cont.) (New Rights)

Right to Correction	Consumers may request any correction of their PI held by a business if that information is inaccurate.
Right to Opt Out of Automated Decision Making Technology	The CPRA authorizes regulations allowing consumers to opt out of the use of automated decision making technology, including "profiling," in connection with decisions related to a consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. **STILL WAITING ON REGULATORY GUIDANCE**
Right to Access Information About Automated Decision Making	The CPRA authorizes regulations allowing consumers to make access requests seeking meaningful information about the logic involved in the decision making processes and a description of the likely outcome based on that process. **STILL WAITING ON REGULATORY GUIDANCE**
Right to Restrict Sensitive PI	Consumers may limit the use and disclosure of sensitive PI for certain secondary purposes, including prohibiting businesses from disclosing sensitive PI to third parties, subject to certain exemptions.

Business Obligations

1. Data Minimization / Retention Periods
2. Expanded Notice Obligations
3. Updating service provider agreements and third party contracts
4. Updating privacy policy and related compliance systems
5. Implementing “reasonable security measures”
6. Audit Obligations (Data Impact Assessments – guidance forthcoming)
7. Respond to universal opt-out mechanism (Global Privacy Controls)

Relationships with External Entities

Service Providers

- Service providers remain entities that process personal information on behalf of a business pursuant to a written contract.
- CPRA clarifies, however, that a service provider may receive the personal information either *directly from* or *on behalf of* the business.

Third Parties

- A third party continues to be a recipient of sales of personal information.
- A third party that offers cross context behavioral advertising can now be the recipient of "sharing" of personal information, as well.

New Term: Contractors

- "Contractor" refers to a person to whom the business makes available a consumer's personal information for a business purpose and pursuant to a written contract. In particular, **contractors are required to certify their understanding and compliance with contractual restrictions.**
- Contractors are **not** data processors.

Notice Obligations

Required notices to consumers:

1. Notice at Collection
2. Notice of Right to Opt Out of Sale and Sharing
3. Notice of Right to Limit Use of Sensitive Personal Information
4. Notice of Financial Incentive
5. Privacy Policy

Sensitive Personal Information

1. Notice at Collection: Disclose the purposes for which categories of both sensitive personal information and personal information are collected or used.
2. Notice of Right to Limit Use of Sensitive Personal Information:
   - Provide a link on homepage titled, “Limit the Use of My Sensitive Personal Information,” which enables consumers to exercise their right.

Right To Opt Out of Sale and Sharing of Personal Information

1. Notice at Collection: Disclose whether collected information is sold or shared.
2. Must provide a Notice with a description of the consumer's right to opt out of the sale or sharing of their personal information.
    - The term "sharing" is defined as the practice of providing information for the purposes of "cross-context behavioral advertising."

Relevant Links To Post On Homepage

- Privacy Policy “California Privacy Notice”
- “Do Not Sell or Share My Personal Information”
- “Limit The Use Of My Sensitive Personal Information”
- *If both selling and/or sharing information AND using Sensitive Personal Information beyond the business purpose permitted uses identified in the CPRA then may post a “combo” link:*
  - Your California Privacy Choices 

Responding and Verifying Consumer Requests

Methods of Submission for Requests to Know

1.A business shall provide two (2) or more designated methods for submitting consumer requests including at a minimum:

a. A Toll-Free Telephone Number

b. If the business operates a website, an interactive webform accessible through the website or mobile application

2. However, if a business operates "exclusively online" and has "a direct relationship" with the consumer from whom it collects information to "only provide an email address for submitting requests."

Timing for Responses to Requests to Know and Requests to Delete

1. Confirm receipt of request **within ten (10) days** and provide information about how the business will process the request.
2. Response to request **within 45 days** (starting from time request is received and regardless of **time required to verify the request)**.
    a. Business must verify consumer's identity prior to fulfilling request
3. If necessary, an **additional 45 days** may be taken but the business must provide the consumer with notice and an explanation of the need for additional time.

Special Rules for Minors

Businesses must notify minors if they intend to sell or share user data for behavioral advertising purposes.

Opt-in consent required for sale or sharing of personal information of consumers 16 or under:

- Between 13-16 – opt in consent from consumer
- Under 13 – opt in consent from parent/guardian

After a consumer under 16 years of age has declined to provide their consent to sell or share their personal information, a business must either wait for another 12 months or wait until the consumer turns 16 before requesting their opt-in consent again.

Handling Employee Data

1	2	3	4
Review your agreements with third-party recipients of personal information of employees.	Implement data subject request protocols and tighten up record retention and data deletion protocols for employee information/ records.	Consider whether and the extent to which you process "sensitive personal information" of employees, including if you use employee monitoring software, and address related CCPA requirements.	Update privacy policy and privacy notices (Employee Notice, Job Applicant Notice) to reflect how you process employee/ HR data.

Miscellaneous Regulations

Training/Recordkeeping

- All individuals responsible for handling consumer inquiries about the business's privacy practices or CPRA compliance shall be informed of all requirements in the CPRA and how to direct consumers to exercise those rights.
- **A business shall maintain records of consumer requests and the business's response for at least 24 months**.
  - Consumer request information may not be used for any other purpose.
  - Aside from this information, businesses are not required to retain personal information solely for the purpose of fulfilling consumer requests.

Penalties/Remedies

California AG Enforcement Action

- $2,500 for unintentional violation
  - 30-day option to cure
- $7,500 for intentional violation
- Penalties paid into State AG Consumer Privacy Fund
- "Actual knowledge" a consumer is under 16 is not required.

Civil Private Right of Action

- Limited to data breach of narrower personal information (as defined in data breach statute – SSN, credit card info, health/medical info, email address in combination with a password or security question that would permit access to an email account)
  - Duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information
- Statutory Damages of $100-$750 per incident per consumer
- OR Actual Damages, whichever is greater

California Privacy Protection Agency (CPPA)

CPRA established California Privacy Protection Agency (CPPA):

- On July 1, 2021, the CPRA transferred rulemaking authority from the California Attorney General to the California Privacy Protection Agency.
- The CPPA was created "to implement and enforce" the CCPA and the CPRA (when it becomes operative).
- The CPPA will be the first privacy agency in the United States devoted solely to consumer data privacy and will have a broad mandate to investigate possible violations of the CPRA, enforce the CPRA through administrative action, and promulgate rules.

Requires a new rulemaking on cybersecurity and privacy:

- The CPPA shall issue regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to (1) perform a cybersecurity audit on an annual basis and (2) submit a risk assessment to the CPPA with respect to their processing of PI.

First CCPA Enforcement Action - SEPHORA

REUTERS® World Business Legal Markets Breakingviews Technology Investigation

Data Privacy | Litigation | Corporate Counsel

3 minute read · August 24, 2022 2:12 PM PDT · Last Updated 5 months ago

Sephora to pay $1.2 mln in privacy settlement with Calif. AG over data sales

By Sara Merken

People enter a Sephora store in New York City, New York, U.S., May 20, 2021. REUTERS/Eduardo Munoz

Failure to inform consumers that they sold data (including via Google Analytics)

Failure to have service provider agreements in place for data disclosure

Failure to honor opt-outs via Global Privacy Control

Global Privacy Control

- Two states require recognition of the Global Privacy Control ("GPC")—namely, California and Colorado.
- GPC is a mechanism by which consumers can exercise their right to "opt out" of a platform or technology processing their personal data for targeted advertising or of the sale of their personal data.

Google Analytics and Restricted Sharing

- Since 2019, Google has offered some of its services on a "restricted data processing" basis
  - When configured as such, Google acted as a service provider
- Starting July 1, 2023 – Google will **no longer** offer restricted data processing for the following services in California:
  - *Any feature that entails uploading customer data for purposes of matching with Google or other data for personalized advertising (e.g., Customer Match)*
  - *Any feature that entails targeting user lists obtained from a third party (e.g., Audience Partner API)*
  - *Any feature that entails creating, adding to, or updating user lists using first-party customer data (e.g., audience building with floodlight tags and audience-expansion features in DV360)*
- **Companies leveraging these services are "selling" or "sharing" personal information and will need to offer consumers an opportunity to opt out.**

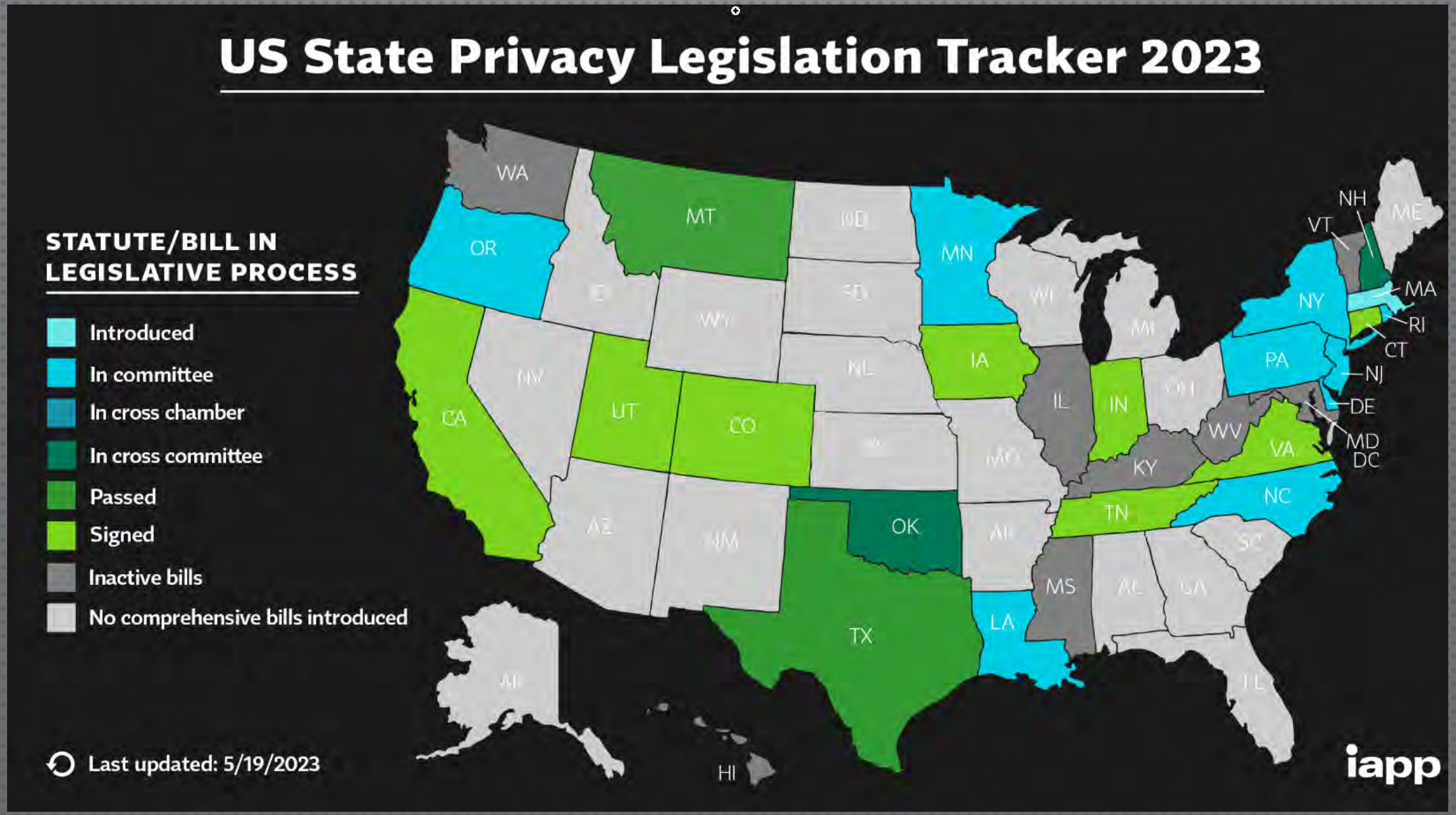
Other States To Consider

Effective Now / July 1, 2023

- Virginia (current)
- Colorado (July 1, 2023)
- Connecticut (July 1, 2023)

Recent New Laws

- Utah (Dec. 1, 2023)
- Texas (July 1, 2024)
- Tennessee (July 1, 2024)
- Montana (Oct. 24, 2024)
- Iowa (Jan. 1, 2025)
- Indiana (Jan. 1, 2026)



Source: US State Privacy Legislation Tracker, IAPP.ORG

Rights Vary Across States

US State Privacy Legislation Tracker 2023

Comprehensive Consumer Privacy Bills

STATE	LEGISLATIVE PROCESS	STATUTE/BILL (HYPERLINKS)	COMMON NAME	CONSUMER RIGHTS: Right to access	Right to correct	Right to delete	Right to opt out of certain processing	Right to portability	Right to opt out of sales	Right to opt in for sensitive data processing	Right against automated decision making	Private right of action	BUSINESS OBLIGATIONS: Opt-in default (requirement age)	Notice/transparency requirement	Risk assessments	Prohibition on discrimination (exercising rights)	Purpose/processing limitation
LAWS SIGNED (TO DATE)																	
California		CCPA	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	X		X		X	X			L	16	X			X
		Proposition 24	California Privacy Rights Act (2020; fully operative Jan. 1, 2023)	X	X	X	S	X	X		X	L	16	X	X	X	X
Colorado		SB 190	Colorado Privacy Act (2021; effective July 1, 2023)	X	X	X	P	X	X	X	X~		S/13	X	X	X	X
Connecticut		SB 6	Connecticut Data Privacy Act (2022; effective July 1, 2023)	X	X	X	P	X	X	X	X~		S/13	X	X	X	X
Indiana		SB 0005	Indiana Consumer Data Protection Act (2023; effective Jan. 1, 2026)	X	X	X	P	X	X	X	X~		S/13	X	X	X	X
Iowa		SF 262	Iowa Consumer Data Protection Act (2023; effective Jan. 1, 2025)	X		X		X	X		X~		S/13	X		X	X
Tennessee		HB 1181	Tennessee Information Protection Act (2023; effective July 1, 2024)	X	X	X	P	X	X	X	X~		S/13	X	X	X	X
Utah		SB 227	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)	X		X	P	X	X				13	X		X	
Virginia		SB 1392	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)	X	X	X	P	X	X	X	X~		S/13	X	X	X	X

Source: US State Privacy Legislation Tracker, IAPP.ORG

What to Consider?

- State Thresholds – Where are you collecting PI?
- Sensitive PI – Opt In States vs. Opt Out States
  - Opt Out – California, Iowa, Utah
  - Opt In – Colorado, Connecticut, Indiana, Tennessee, Virginia
- Risk Assessments (California, Colorado, Connecticut, Indiana, Tennessee, Virginia)
- Right to Appeal (Colorado, Virginia, Connecticut, Texas)

Recent Trends in Privacy Litigation

- California Invasion of Privacy Act ("CIPA")
- Video Privacy Protection Act ("VPPA")

California Invasion of Privacy Act ("CIPA")

- CIPA prohibits businesses from using devices to "eavesdrop" on or "wiretap" a conversation without consent
- New wave of lawsuits against session recording technologies and chatbot functions
- Statutory penalty of $5,000 per violation
- Recent dismissals at the pleading stage:
  - Website operator can use a chat feature to enable and store a conversation with one of its users without "eavesdropping" on that conversation
  - Third-party vendor can collect and process personal information only on behalf of the business's operation and benefit

Video Privacy Protection Act ("VPPA")

- VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifiable information" of a "consumer," such as by publishing a subscriber's video watching history
- New wave of lawsuits against businesses that stream videos on their websites using ad targeting cookies (i.e., Meta Pixel)
- Statutory penalty of $2,500 per violation
- Defendants have raised First Amendment challenges to VPPA:
  - VPPA prohibits certain noncommercial speech, such as personal conversations of a video tape service provider
  - VPPA limits the distribution of sharing information of public interest

Video Privacy Protection Act ("VPPA")

- Whether the defendant is a "video tape service provider"
- Whether the data at issue contains "personally identifying information"
- The extent to which statutory exceptions or exemptions may apply;
- Potential limitations on the types of remedies available;
- Whether the plaintiff consented to the challenged data practices; and
- Whether any of these issues can be adjudicated on a class wide basis

How Can Businesses Reduce the Risk of Privacy Litigation?

- Understand how websites uses tracking analytics and pixels, including Meta Pixel, Google Analytics, and other software
- Implement consumer notification requirements and opt-in or opt-out mechanisms for consent
- Ensure compliance with privacy laws and regulations when introducing new technologies that interact with consumers

Data Breach: Numbers

- Number of companies affected in the U.S. in 2022: ~1800
- Number of Americans affected in the U.S. in 2022: 422 million

Source: Statista, www.statista.com

Data Breach: Costs

- Global average cost of data breach in 2022: $4.35 million
- U.S. average cost of data breach in 2022: $9.44 million
- Cost higher where there is remote work
- Most expensive industries for data breach
  - Healthcare
  - Finance
  - Technology
- Cost lower where company has Incident Response Plan

Source: IBM 2022 Cost of a Data Breach Report, https://www.ibm.com/reports/data-breach

Data Breach: Preparation

- Incident Response Plan
- Cyber insurance
- Incident response team
  - Internal
  - External
    - Outside counsel
    - Forensics investigator
    - Communications
- Practice

Key Questions/Action Items For Businesses Regarding Preparedness (cont.)

- Assess data flows and privacy practices (including for sensitive data, data sales and website analytics/cookies)
- Prepare required updated notices/privacy policies (including employee and B2B notices)
- Implement service provider or third-party agreements for disclosure of personal information
- Processes/infrastructure in place for handling and responding to consumer requests
  - Prepare process for verifying consumers and templates for responses to requests
  - Training for employees responding to consumer requests and documenting responses
- Data breach response plans/protocols up to date
- Review cybersecurity insurance
- Monitor new laws (state laws, biometric laws, etc.) in jurisdictions where you do business
- Contact us with questions or assistance

Thank You for Attending

Please direct any questions to Scott Hall and our privacy team.

Scott C. Hall
Partner
shall@coblentzlaw.com

Mari S. Clifford
Associate
mclifford@coblentzlaw.com

Sabrina A. Larson
Partner
slarson@coblentzlaw.com

Amber Leong
Associate
aleong@coblentzlaw.com

Bina Patel
Associate
bpatel@coblentzlaw.com