

iapp REPORT

US State Comprehensive Privacy Laws

2022 LEGISLATIVE SESSION

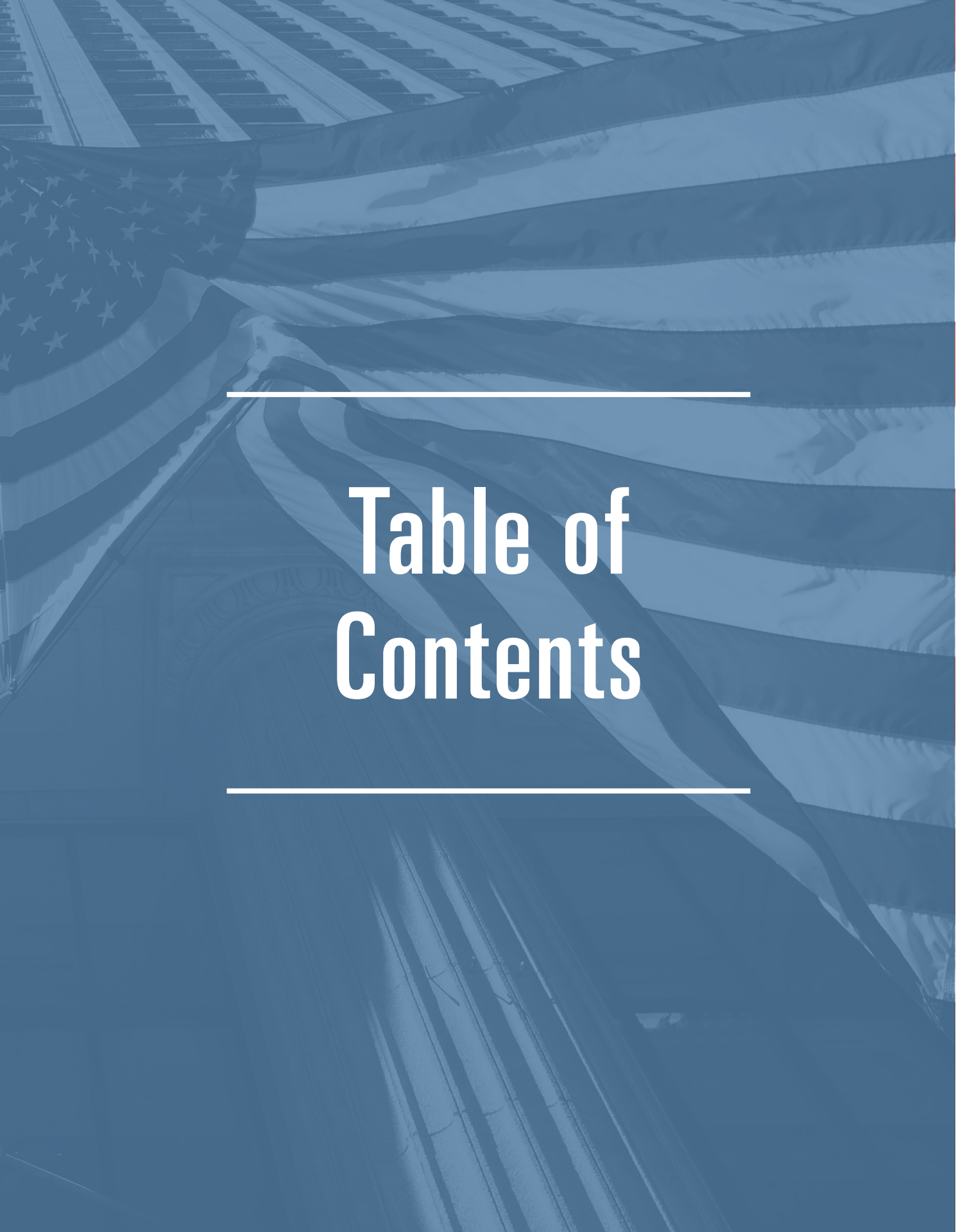


Table of Contents

What's inside?

Overview.....	3
Relevant definitions.....	9
Exemptions.....	12
Consumer rights.....	14
Business/controller obligations.....	18
Enforcement.....	26
Contacts.....	29

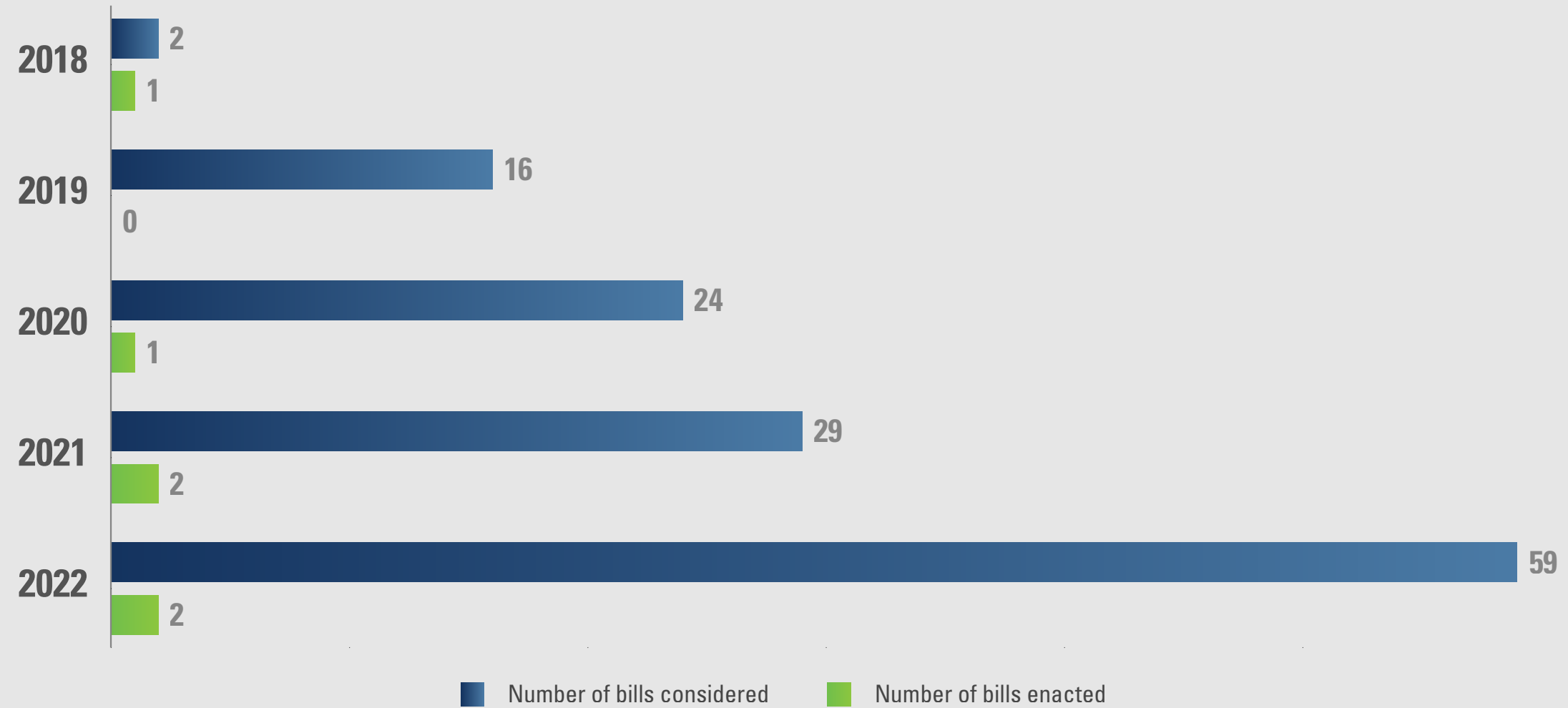
Overview

Keeping pace with US state privacy legislation

Each year since the passage of the California Consumer Privacy Act, the first comprehensive state law, in 2018, the number of proposed U.S. state privacy bills has increased. The IAPP aims to keep privacy professionals informed when states introduce comprehensive privacy bills, when those bills progress into laws, what rights they offer consumers and what obligations they require from organizations.

In 2018, two bills were introduced in the U.S. and one, the CCPA, became law by ballot initiative in California. In 2019, 15 bills were introduced throughout the U.S. Of the 24 bills introduced in 2020, one was enacted, this time in the form of an update to California's law. In 2021, two of 29 introduced bills were enacted in Virginia and Colorado. And again in 2022, two of the 59 introduced bills became law in Utah and Connecticut. Understandably, balancing compliance with passed laws, while keeping track of newly introduced comprehensive privacy bills can be overwhelming for privacy professionals. The IAPP's [US State Privacy Legislation Tracker](#) provides a quick snapshot of new bills as each state's legislative session begins. This report provides a summary of relevant terms, applicability, exemptions, consumer rights, business obligations and enforcement duties for each of the five passed laws to date.

The growth of US state privacy legislation



States with enacted laws



CALIFORNIA

- ☑ California Consumer Privacy Act (effective Jan. 1, 2020)
 - As amended by the California Privacy Rights Act (fully effective Jan. 1, 2023)



VIRGINIA

- ☑ Virginia Consumer Data Protection Act (effective Jan. 1, 2023)



UTAH

- ☑ Utah Consumer Privacy Act (effective Dec. 31, 2023)



COLORADO

- ☑ Colorado Privacy Act (effective July 1, 2023)



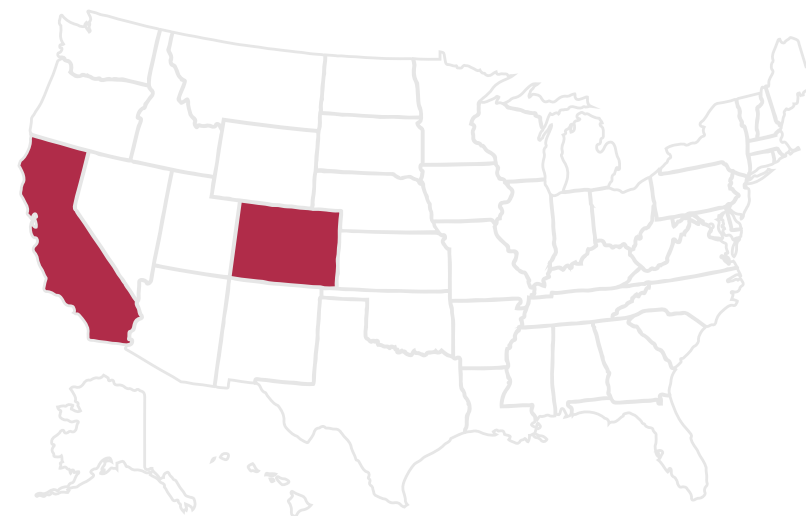
CONNECTICUT

- ☑ Connecticut Personal Data Privacy and Online Monitoring Act (effective July 1, 2023)

Scope

This report analyzes similarities and differences between the five enacted comprehensive state privacy laws. These states have continued to propose updates to their passed laws within their definitions, scope and enforceability. As such, guidance continues to change with future amendments. Colorado and California, in particular, have explicitly granted rulemaking authority for privacy laws to their respective attorneys general.

States with rulemaking authority



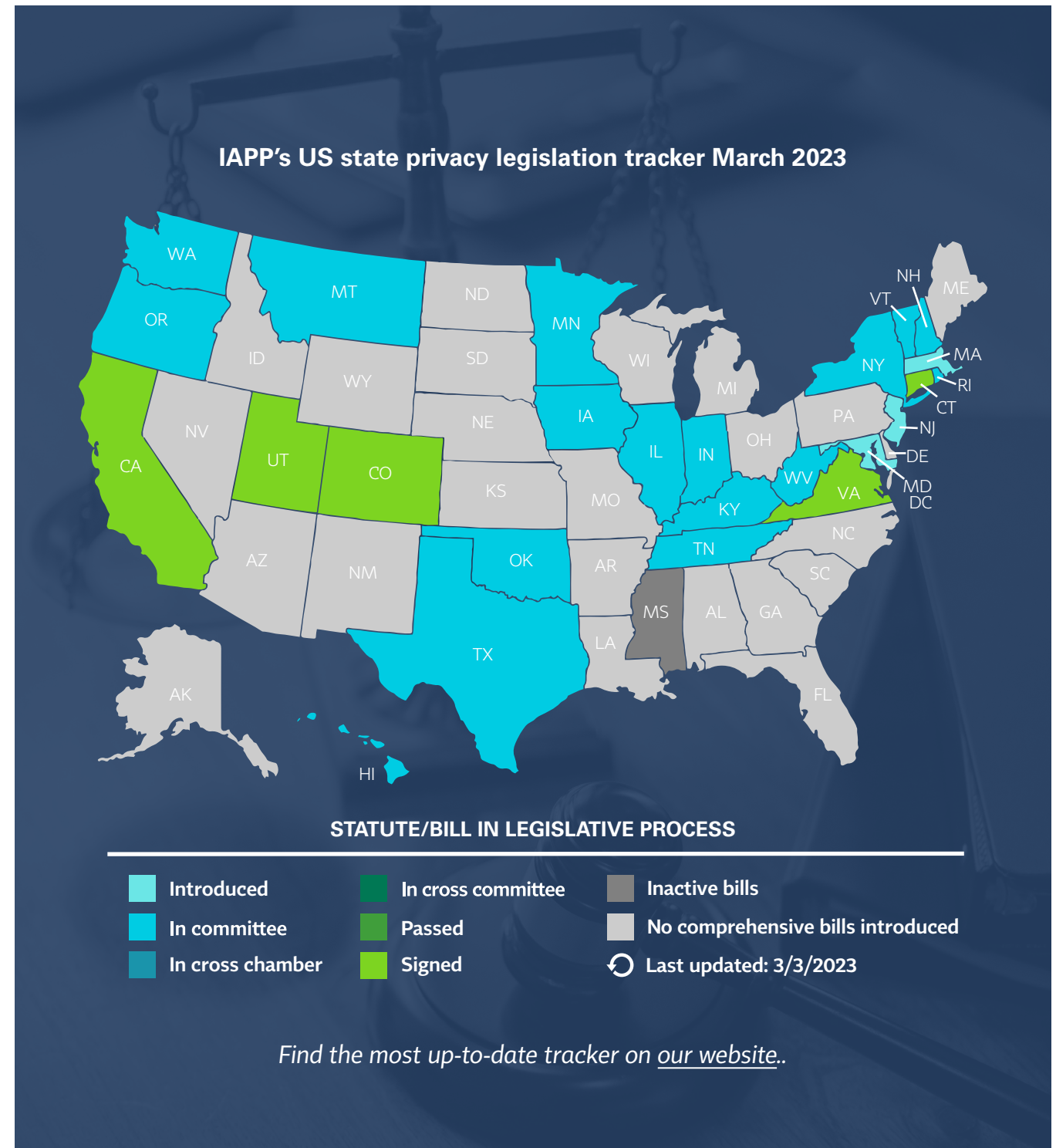
CALIFORNIA AND COLORADO

The current US State privacy landscape

California enacted the CCPA in 2018, which was amended by the California Privacy Rights Act in 2020. The CCPA went into effect Jan. 1, 2020 and the CPRA amendment went into effect Jan. 1, 2023. Both enacted in 2021, the Virginia Consumer Data Protection Act also went into effect Jan. 1, 2023 and the Colorado Privacy Act will be effective July 1, 2023. Finally, the Connecticut Personal Data Privacy and Online Monitoring Act and the Utah Consumer Privacy Act were passed in 2022, and will go into effect July 1, 2023 and Dec. 31, 2023, respectively.

So far, the U.S. has seen two different approaches to state consumer privacy laws. While California followed its own approach, the other four states, at least initially, generally based

their laws on a version of the yet-to-pass Washington Privacy Act. For example, California uses the term business, where the other states use the term controller for certain entities subject to the law, which may include an individual, corporation, business trust, non-profit, and other legal and commercial entities. At this point California is also the only state requiring notice at collection. The CCPA initially did not address sensitive data, but this was updated by the CPRA amendments. With the CPRA amending the CCPA, California is now the only state that gives consumers the right to limit the use and disclosure of sensitive personal information. Unlike the other states, California has a dedicated privacy agency, the California Privacy Protection Agency.



Two different approaches

CALIFORNIA	VS.	VIRGINIA, COLORADO, UTAH AND CONNECTICUT
Business	▶	Controller
Notice at collection	✕	N/A
Sensitive data initially not included	▶	Sensitive data included
Right to limit use of sensitive data	✕	N/A
California Privacy Protection Agency	✕	N/A

Applicability of US state comprehensive privacy laws

	CCPA	CPRA	VIRGINIA	COLORADO	UTAH	CONNECTICUT
JURISDICTIONAL THRESHOLD	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state & \$25M in annual revenues	Doing business in the state
AND ONE OF THE FOLLOWING:						
REVENUE THRESHOLD	>\$25M	>\$25M				
PROCESSING THRESHOLD	50K+ consumers	100K+ consumers	100K+ consumers	100K+ consumers	100K+ consumers	100K+ consumers (excludes payment data)
SALE THRESHOLD	50% of revenue from selling data	50% of revenue from selling or sharing data	50% of revenue from selling data & data of 25K consumers	Any revenue or discount from selling data & data of 25K consumers	50% of revenue from selling data & data of 25K consumers	25% of revenue from selling data & data of 25K consumers

Relevant definitions

Defining privacy

The five states with comprehensive consumer privacy laws each include important terms like consumer, personal data and sale. Because each law provides its own interpretation of those terms, it is important for privacy professionals to understand the differences between definitions across state lines.

Terms with varying definitions in US state comprehensive privacy laws



SALE



PERSONAL DATA



CONSUMER



SENSITIVE PERSONAL DATA

Sale and consumer

The term sale is defined as “an exchange of personal data for monetary or other valuable consideration” in California, Colorado and Connecticut, while the definition only includes “monetary consideration” in Virginia and Utah. Of the existing state privacy laws, four define consumer as a resident of the state and exclude parties acting in a commercial or employment context. But in California consumer also applies to employees.



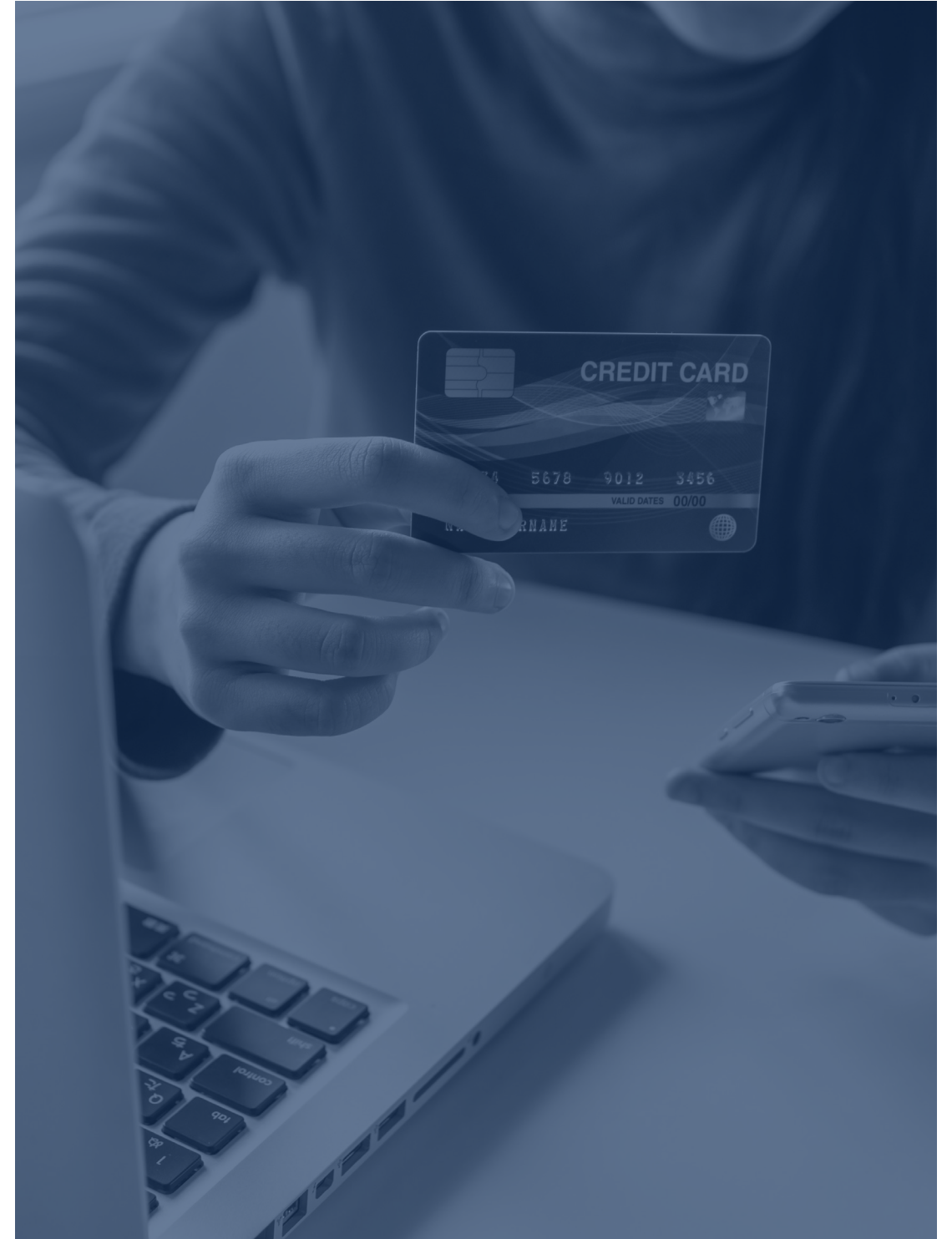
SALE

- ▣ Sale defined as “an exchange of personal data for...”
 - ▣ “...**monetary or other valuable consideration**” (California, Colorado and Connecticut).
 - ▣ “...**monetary consideration**” only (Virginia and Utah).



CONSUMER

- ▣ Most define **consumer** to exclude those acting in a commercial or employment context
 - ▣ California does **not** exclude such individuals and exemptions for this data are set to expire Jan. 1, 2023.



Personal data and sensitive personal data

The passed laws all exclude publicly available information and deidentified data from their definitions of personal data, and California and Utah additionally exclude aggregate data. All five states include consumer race or ethnic origin, religious beliefs, genetic data, biometric data, health data and sexual orientation in their definitions of sensitive personal data. Each law further clarifies biometric data, as seen by Virginia's exclusion of facial recognition technology data from its definition. The Colorado Privacy Act does not currently define the term, but defers to the attorney general to define the term during its rulemaking activities. The Colorado attorney general, in turn,

proposed [draft rules](#) that include definitions of biometric data and biometric identifiers similar to those provided in other passed state privacy laws. In Virginia, Colorado and Connecticut, sensitive data also includes personal data from known children. California, Colorado and Connecticut include consumers' sex lives in the definition. All the states, except California, include citizenship and immigration status and all but Colorado include precise or specific geolocation data in their definitions of sensitive personal data. Lastly, the CPRA includes a few additional types of personal data: philosophical beliefs, union membership, account login information, government-issued identifications and contents of mail, email or text messages.



PERSONAL DATA

- ▢ All exclude **publicly available information** and **deidentified data** from the definition of **personal data**.
 - ▢ California and Utah also exclude **aggregate data**.



SENSITIVE PERSONAL DATA

- ▢ All define **sensitive personal data** to include **race or ethnic origin, religious beliefs, genetic data, biometric data, health data and sexual orientation**.
 - ▢ Virginia, Colorado and Connecticut include **personal data from a known child**.
 - ▢ Most include **precise geolocation data**.
 - ▢ California includes additional categories, such as **philosophical beliefs** and the **contents of a consumer's mail, email, and text messages**.



Exemptions

The two main exemptions

The five passed state privacy laws generally have two types of exemptions: one at the entity level and one at the data level. Most of the entity-level exemptions include government entities, nonprofits, and entities already regulated by the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act. There are two exceptions: Colorado does not provide an entity-level exemption for nonprofits or HIPAA-regulated entities and California does not provide an entity-level exemption for GLBA-regulated entities. Virginia, Utah and Connecticut exempt higher education institutions, while Colorado and Connecticut specifically exempt registered national securities associations.

All five states exempt data regulated under HIPAA, GLBA, the Fair Credit Reporting Act and the Driver's Privacy Protection Act. These exemptions also come with some exceptions. Colorado and Utah only exempt GLBA regulated data if the entity is GLBA compliant. Virginia, Utah and Connecticut only exempt DPPA regulated data if the entity is DPPA compliant. All the states except Colorado exempt data regulated by the Family Educational Rights and Privacy Act, and all but California exempt employee and commercial business-to-business data.

US state comprehensive privacy law exemptions



ENTITY-LEVEL

- ▣ Most exempt:
 - ▣ **Government.**
 - ▣ **Nonprofits.**
 - ▣ **HIPAA regulated entities.**
 - ▣ **GLBA regulated entities.**
- ▣ **Institutions of higher education** exempt under Virginia, Utah and Connecticut.
- ▣ **Registered national securities associations** exempt under Colorado and Connecticut.



DATA-LEVEL

- ▣ All generally exempt data regulated under:
 - ▣ **HIPAA.**
 - ▣ **GLBA.**
 - ▣ **FCRA.**
 - ▣ **DPPA.**
- ▣ Most exempt **FERPA regulated data.**
- ▣ Most exempt **employee data** and **commercial business-to-business data.**



Consumer rights

Access, portability, deletion, correction and opt-out

The CCPA set the standard for rights consumers can expect to be protected by other state privacy laws. These consumer rights include the right to access data, port data in a noncumbersome way, delete data, usually after authenticating identity, correct data, and opt out of sales or certain processing. All five states provide consumers the right to access their personal data, with Colorado and Connecticut providing an exception to this right if it would require a covered entity to reveal a trade secret. The right to data portability is not consistently guaranteed. Virginia and Utah limit consumers' right to obtain a portable copy of their data to consumer-provided data only.

Similarly, the right to deletion comes with certain exceptions across states. In California and Utah, consumers have the right to delete only consumer-provided data, while the remaining three states afford the right to delete any personal data the covered entity has concerning the consumer. Virginia passed further amendments that provide an exemption to this right where personal data was collected from a third-party source. All states but Utah provide consumers with the right to correct inaccurate personal data the covered entity maintains about the consumer. Finally, when it comes to opt-out rights, all states provide consumers the right to opt out of sales and some form of targeted advertising. All states but Utah also provide the right to opt out of profiling, and only California affords the right to limit the use and disclosure of sensitive personal information. However, all states but California and Utah provide the right to opt in to sensitive data processing.

Consumer rights



ACCESS AND PORTABILITY

ACCESS

- ☑ All states generally give consumers a **right to access** their data.
 - ☐ Trade secrets are explicitly excluded in Colorado, Connecticut and California.



PORTABILITY

- ☑ Consumers have the **right to data portability** for:
 - ☐ Only consumer-provided data (Virginia and Utah).
 - ☐ Any personal data the business/controller has concerning the consumer (California, Colorado and Connecticut).

Consumer rights

DELETION AND CORRECTION



DELETION

- ☑ Consumers have the **right to delete**:
 - ☐ Only consumer-provided data (California and Utah).
 - ☐ Any personal data the business/controller has concerning the consumer (Virginia, Colorado and Connecticut).



CORRECTION

- ☑ Most states give consumers a **right to correct** inaccurate personal data.
 - ☐ Only Utah does not provide this right.

Consumer rights

OPT-OUT RIGHTS



	CALIFORNIA	VIRGINIA	COLORADO	UTAH	CONNECTICUT
SALES	✔	✔	✔	✔	✔
SHARED/TARGETED ADVERTISING	✔ (CPRA)	✔	✔	✔	✔
PROFILING	✔ (CPRA, by regulation)	✔	✔	✘	✔

Note: there are definitional differences between the laws (e.g., sale)

Business/ controller obligations

Creating accountability for businesses

Comprehensive state privacy laws are not only passed to provide consumers with commercial data rights, but also to create accountability measures for businesses — and nonprofits in the case of Colorado — that collect, use, process, own, manage and discard consumer data. State privacy laws include requirements for processing, treatment of children’s data, transparency, data security, data protection assessments, nondiscrimination and consumer requests.

Business requirements under US state privacy laws



PROCESSING
RESTRICTIONS



TREATMENT OF
CHILDREN'S DATA



TRANSPARENCY



DATA SECURITY



DATA PROTECTION
ASSESSMENTS



NONDISCRIMINATION



CONSUMER REQUESTS

Requirements of covered entities

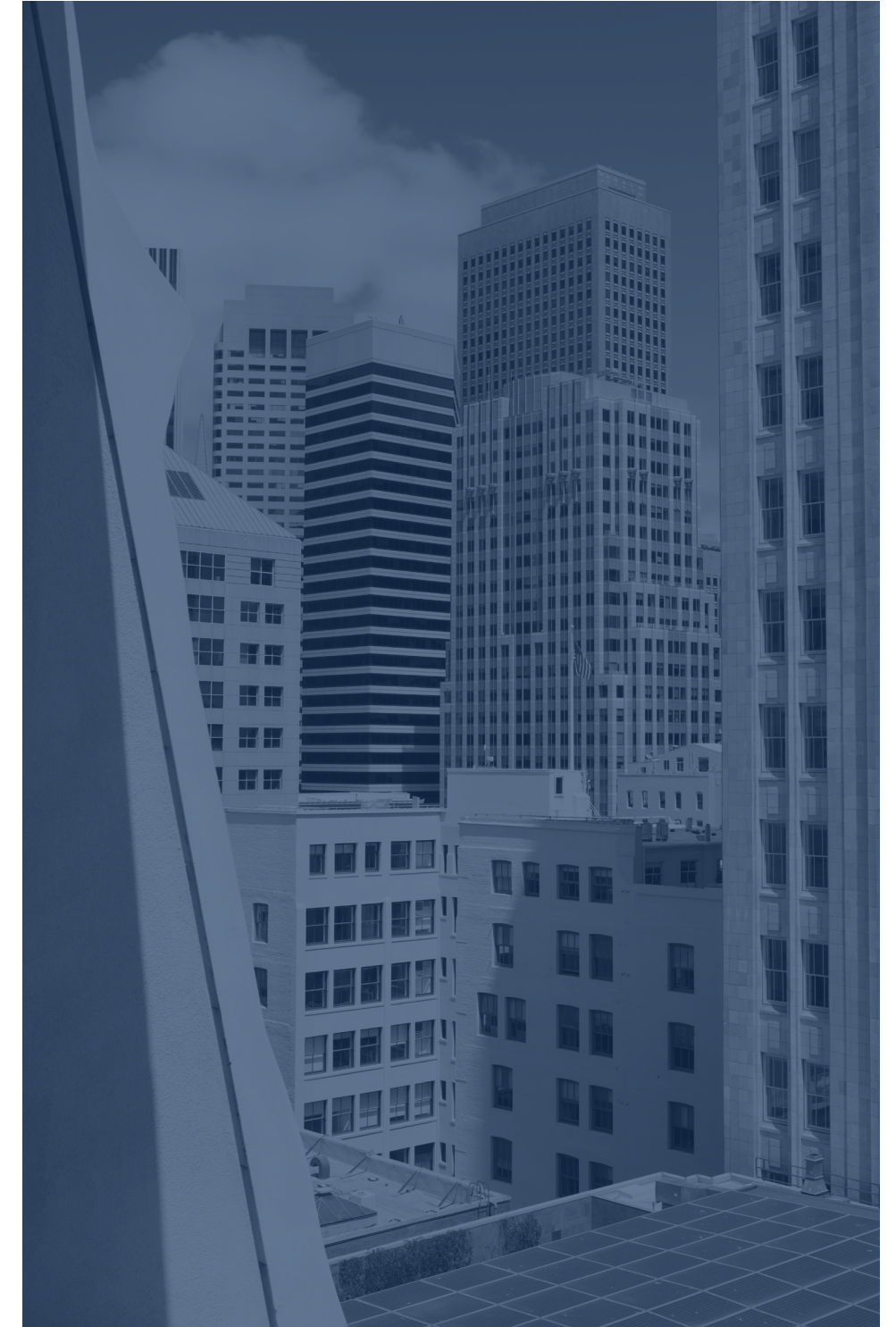
California's notice-at-collection requirement ensures each covered entity gives consumers notice about which categories of personal information are collected and the business purposes for doing so, along with a link to its "Do Not Sell" page and privacy policy. Virginia, Colorado and Connecticut require consumer consent before processing sensitive data, and Utah specifically requires covered entities to provide notice and an opportunity to opt out of sensitive data processing. Interestingly, California and Connecticut require consent to sell, share or process the data of consumers under age 16 for targeted advertising purposes, while Virginia, Colorado, Utah and Connecticut require parental consent to process the data of consumers under age 13.

All five states generally require covered entities to provide privacy notices including information about how they use and process consumer data, but there is variation regarding requirements to maintain reasonable data security practices. [California](#) relates its reasonable security to practices a covered entity takes that would be appropriate to the nature of the information requiring protection from unauthorized access, destruction, use, modification or disclosure. [Virginia](#) and [Connecticut](#) go one step further to require "reasonable administrative, technical, and physical data security practices" to be appropriate to the volume and nature of the personal data at issue. [Utah's](#) reasonable data security practices must not only protect the confidentiality and integrity of the personal data, but also reasonably reduce any foreseeable risks of harm to consumers, in an appropriate way for the controller's business size, scope, and type, and

the volume and nature of the personal data. On the other end of the spectrum, [Colorado](#) places its explanation of reasonable security practices within a rule that describes the duty of care. The text of this rule continues to be edited as a part of the rulemaking process.

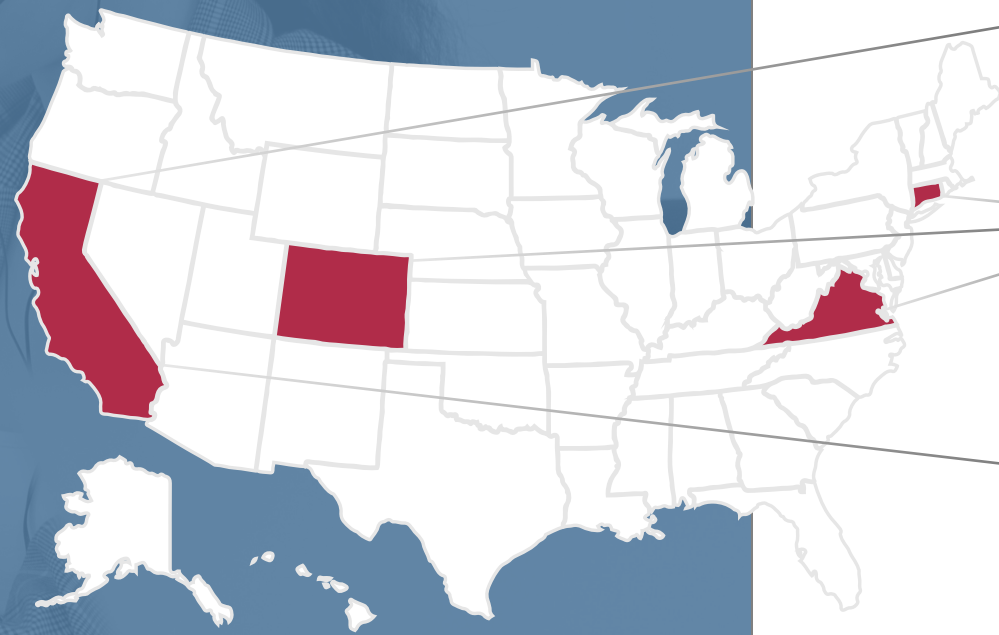
Colorado, Virginia and Connecticut require covered entities to conduct data protection assessments for certain types of processing activities, like selling or processing personal data. Most states provide general parameters for responding to consumer requests but leave the processing of those requests up to the covered entity's discretion. Consumers must verify their identities when submitting requests to covered entities in Virginia, Colorado and Utah, but California and Connecticut do not require verification for opt-out requests. All five states have a 45-day response period during which covered organizations are expected to respond to consumer requests, with the ability to extend the period if reasonably necessary. For opt-out requests, California and Connecticut specify a 15-day response period. Further, Virginia, Colorado and Connecticut have appeals process requirements to help consumers contact their state attorneys general if they are dissatisfied with appeal results.

A recent development among state privacy laws has been the recognition of universal opt-out mechanisms like the Global Privacy Control. Recent California enforcement pointed to the recognition of universal opt-out mechanisms. Recognition will be required under Colorado's act beginning July 1, 2024, and Connecticut's act beginning Jan. 1, 2025.



Business/Controller obligations

PROCESSING RESTRICTIONS



☐ California has a **notice-at-collection** requirement.

☐ Virginia, Colorado and Connecticut require **consent to process sensitive personal data**, as defined by each law.

☐ California (CPRA) limits the **use and disclosure of sensitive data**.

Business/Controller obligations

TREATMENT OF CHILDREN'S DATA



UNDER 13 YEARS OLD

- ☒ Consent required to **process** data:
 - Virginia, Colorado, Utah and Connecticut.



UNDER 16 YEARS OLD

- ☒ Consent required to **sell, share or process data** for **targeted advertising** purposes:
 - California and Connecticut.

Business/Controller obligations

TRANSPARENCY AND DATA SECURITY



TRANSPARENCY

- ▣ All states generally require privacy notices with certain information.



DATA SECURITY

- ▣ All states generally require businesses/controllers to maintain reasonable data security.

Note: there is variation among the laws for what each obligation requires

Business/Controller obligations

DATA PROTECTION ASSESSMENTS AND NONDISCRIMINATION



ASSESSMENTS

- ☒ Most states generally require controllers to conduct **data protection assessments** for certain types of processing activities.
 - ☐ Utah does not require these assessments.



DISCRIMINATION

- ☒ All states generally **prohibit discrimination** against consumers for exercising their rights.

Business/Controller obligations

RESPONDING TO CONSUMER RIGHTS REQUESTS



AUTHENTICATION

- ☑ Generally required for all consumer requests, **except opt-out requests in California and Connecticut.**



UNIVERSAL OPT-OUT PREFERENCE SIGNALS

- ☑ California (recognition required by regulation).
- ☑ Recognition **will be** required by Colorado July 1, 2024 and Connecticut Jan. 1, 2025.



APPEALS PROCESS

- ☑ Virginia, Colorado and Connecticut.



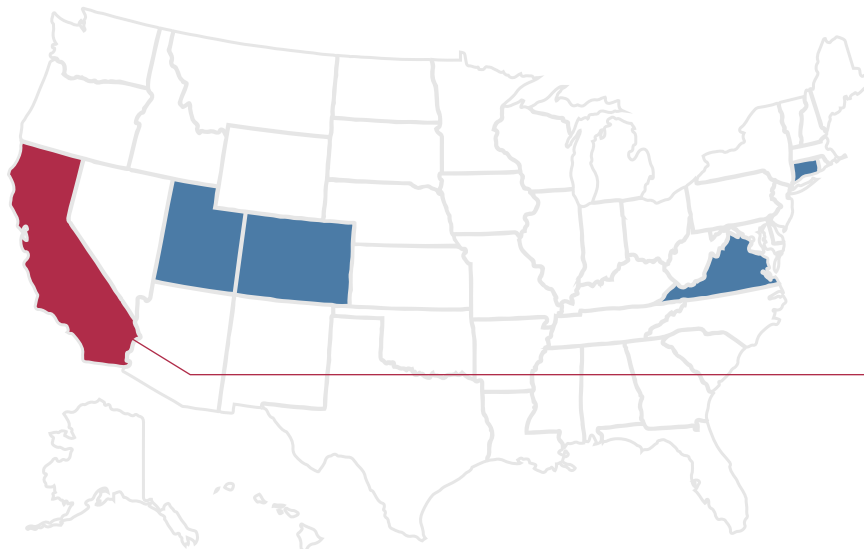
TIMING

- ☑ All states generally require a 45 day response period with discretionary extension.

Data processing agreements

All five states generally require data processing agreements between controllers and processors, or service providers as they are called under California law. California also requires these agreements for third parties under certain circumstances. There is variation among the laws with respect to what should be required by the data processing agreements. Notably, in comparison with many country-level laws, there are no restrictions on international data transfers in U.S. state consumer privacy laws.

Data processing under US state privacy laws



→ All 5 states generally require data processing agreements between **controllers** and **processors**.

California has specific contractual requirements for **contractors, service providers** and **third parties**.





Enforcement

Enforcement authority, cure periods and civil penalties

All five states utilize their attorneys general for enforcement purposes, but California placed joint enforcement authority in the attorney general and the California Privacy Protection Agency created by the CPRA. Colorado placed joint enforcement authority in its attorney general and district attorneys. As of now, only California allows a limited private right of action only for data breaches. The states generally provide a cure period, during which covered entities found to have privacy act violations can remedy issues before facing enforcement. Virginia and Utah offer a 30-day cure period, while Colorado and Connecticut currently offer a 60-day cure period. This feature is no longer provided in California and is due to sunset in Colorado and Connecticut on Jan. 1, 2025. Covered entities that violate their respective state laws can face fines of USD2,500 per violation or USD7,500 per intentional violation or violation involving consumers under 16 in California, up to USD7,500 per violation in Virginia and Utah, USD5,000 per willful violation in Connecticut, and up to USD20,000 per violation in Colorado.

Enforcement of US privacy laws



ENFORCEMENT AUTHORITY

- **Attorneys general** in all states, but joint enforcement authority in:
 - California, with **California Privacy Protection Agency**.
 - Colorado, with **district attorneys**.
- **Private right of action** available only in California and limited to data breaches.



CURE PERIODS

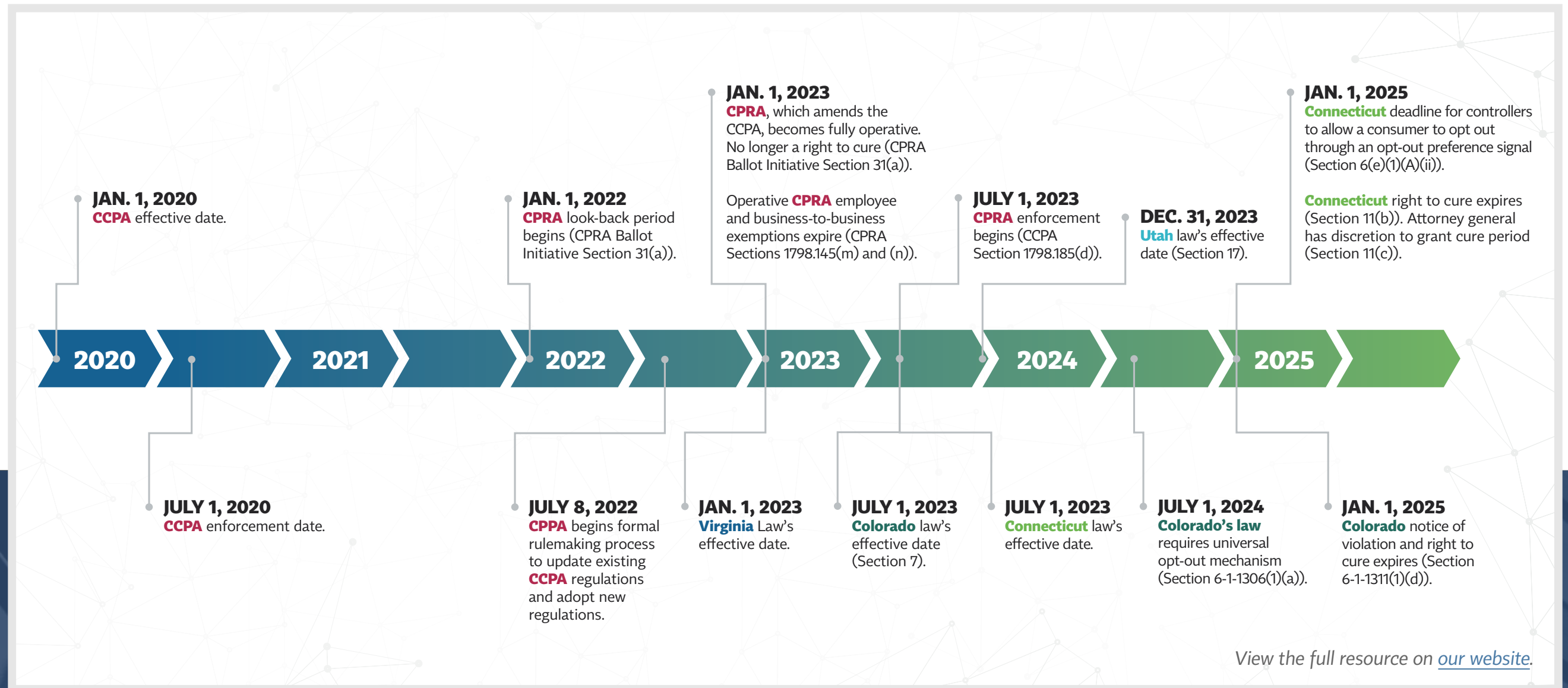
- **30 days:** California (CCPA), Virginia and Utah.
 - **60 days:** Colorado and Connecticut.
- Note: the right to cure provisions will sunset in California (CPRA), Colorado and Connecticut*



CIVIL PENALTIES

- Fines per violation range from a maximum of **\$2,500 to \$20,000**.

Key dates from US state comprehensive privacy laws



Contacts

Anokhy Desai, CIPP/US, CIPT

Westin Fellow, IAPP

adesai@iapp.org

Taylor Kay Lively, CIPP/US *

Data Privacy Attorney, Husch Blackwell

taylorkay.lively@huschblackwell.com

Cathy Cosgrove

Former Legal Research Fellow, IAPP

Joe Jones

Research & Insights Director, IAPP

jjones@iapp.org

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media



**The work on this report was done solely in her previous capacity as Westin Fellow at the IAPP.*

Published March 2023.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2023 International Association of Privacy Professionals. All rights reserved.