MAYER | BROWN

All the Buzz:

The Latest Developments for Emerging & Tech Companies @ Silicon Slopes

Utah Consumer Privacy Act: What You Need to Know

Agenda

1. Overview of the Utah Consumer Privacy Act
2. How the UCPA Compares with other State Privacy Laws
3. Federal Privacy Law Update
4. Preparing for the New Law: Privacy Compliance
5. Privacy Tips for Deal Makers

Overview of the Utah Consumer Privacy Act (UCPA)

MAYER | BROWN

UCPA-Utah Consumer Privacy Act

- Who does the law apply to?
  - Entities that:
    - (1) conduct business in Utah or target products and services to Utah residents,
    - (2) have annual revenue of at least $25 million, and
    - (3) meet one of two threshold requirements:
      - (a) Annually control or process the personal data of 100,000 or more Utah residents ("consumers"); *or*
      - (b) Derive over 50 percent of gross revenue from the "sale" of personal data and control or process personal data of 25,000 or more consumers.

UCPA-Utah Consumer Privacy Act

- Key Definitions
  - "Consumers" are individuals who are residents of Utah acting in an individual or household context. "Consumer" does not include individuals acting in an employment or commercial (business-to-business) context.
  - "Personal Data" is information linked or reasonably linkable to an individual. It does not include de-identified data, aggregated data or publicly available information.

UCPA-Utah Consumer Privacy Act

- Who is exempt?
  - Government Entities
  - Tribes
  - Institutions of Higher Education
  - Nonprofit Corporations
  - Healthcare Organizations (Covered by HIPAA)
  - Financial Institutions (Covered by GLBA)
  - Consumer Reporting Agencies subject to FCRA

UCPA-Utah Consumer Privacy Act

- When will the law take effect?
  - UCPA was signed on March 24, 2022
  - Becomes effective on December 31, 2023

UCPA-Utah Consumer Privacy Act

- What rights does the law give consumers?
  - The right to access and delete certain personal data.
  - The right to obtain a copy of the consumer's personal data.
  - The right to opt out of the collection and use of personal data.
  - The right to know what personal data a business collects, how the business uses the data, and whether the business sells the personal data.

UCPA-Utah Consumer Privacy Act

- What does the law require of businesses?
  - Must safeguard the personal data of consumers.
  - Accept and comply with a consumer's request to access or delete personal data or otherwise exercise their rights under the UCPA.
  - Provide a clear privacy notice.
  - Contracts with Processors establishing the detail of the processing.

UCPA-Utah Consumer Privacy Act

All the Buzz

- What does the Privacy Notice need to include:
  - Categories of personal data processed
  - Purposes for the processing
  - How consumers can exercise their rights under the law
  - Categories of personal data that the controller shares with third parties
  - Categories of third parties with whom the controller shares personal data

UCPA-Utah Consumer Privacy Act

All the Buzz

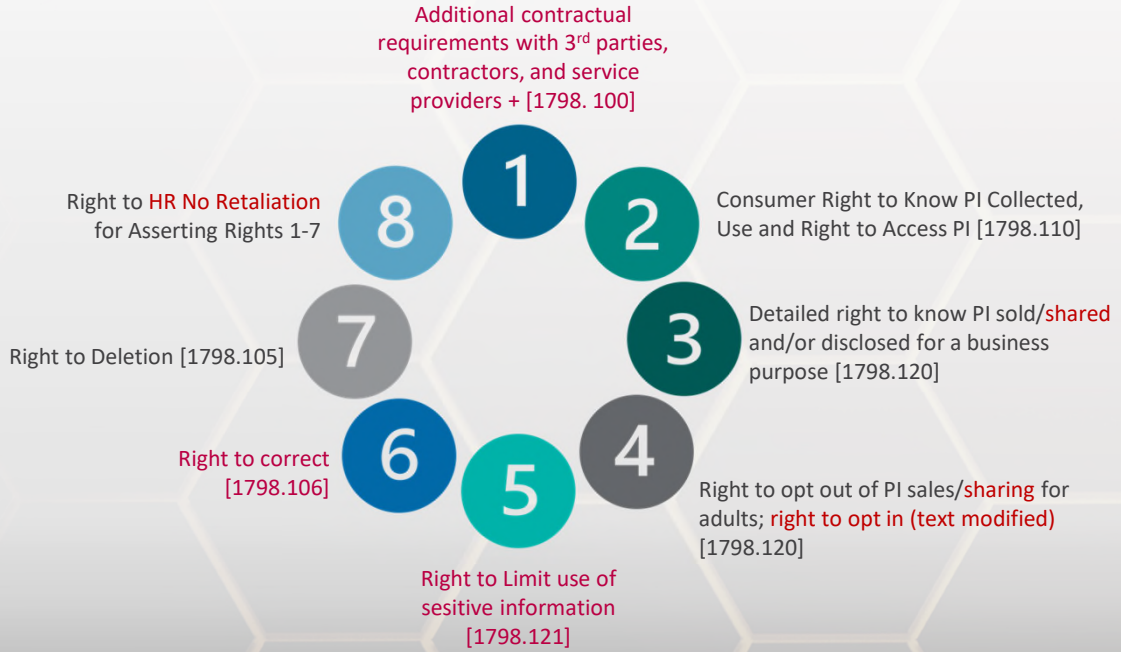
- How will the UCPA be enforced?
  - Division of Consumer Protection will investigate complaints regarding the processing of personal data.
  - Attorney General may take enforcement action and impose penalties.
  - AG must give businesses 30 days to cure any violations.
  - Penalties of up to $7,500 per violation.
  - No private right of action.

UCPA Compared to Other State Laws

MAYER | BROWN

Overview of Compliance *(cont'd)*

California Privacy Rights Act (2023)



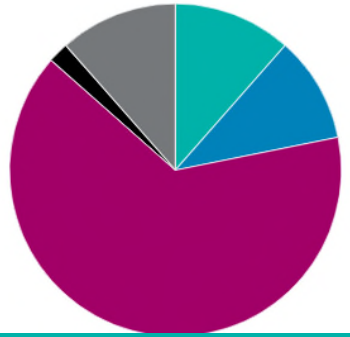
New Legal Developments: CPRA

- B2B and human resources data now within scope of legal regimes

CCPA Litigation Trends

- Over 230+ lawsuits
- Majority triggered by data breaches
- Data sale/disclosure issues also implicated

Triggering Actions



- Privacy Notice
- Data Sale/Disclosure
- Data Breach
- Data Rights/Requests
- Miscellaneous

To date, there have been

230+

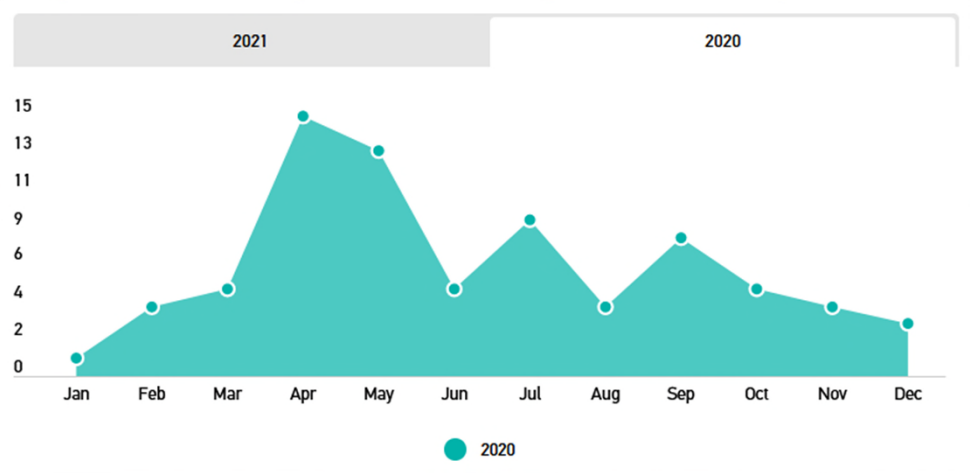
CCPA-related actions filed.

CCPA Litigation Trends 2020

All the Buzz

Month Filed

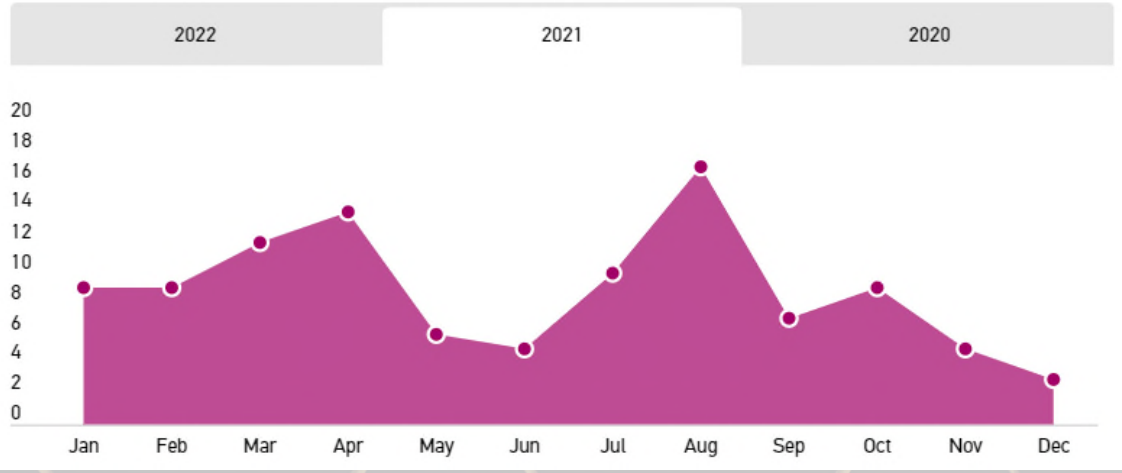
This graph indicates the months where CCPA cases were filed. We see a spike in filings in Q1 2020 and another spike in the Fall of 2020. The Q1 spike is likely due to the timing of when the CCPA went into effect. The increase in the Fall was likely an anticipation of the CPRA going on the ballot.



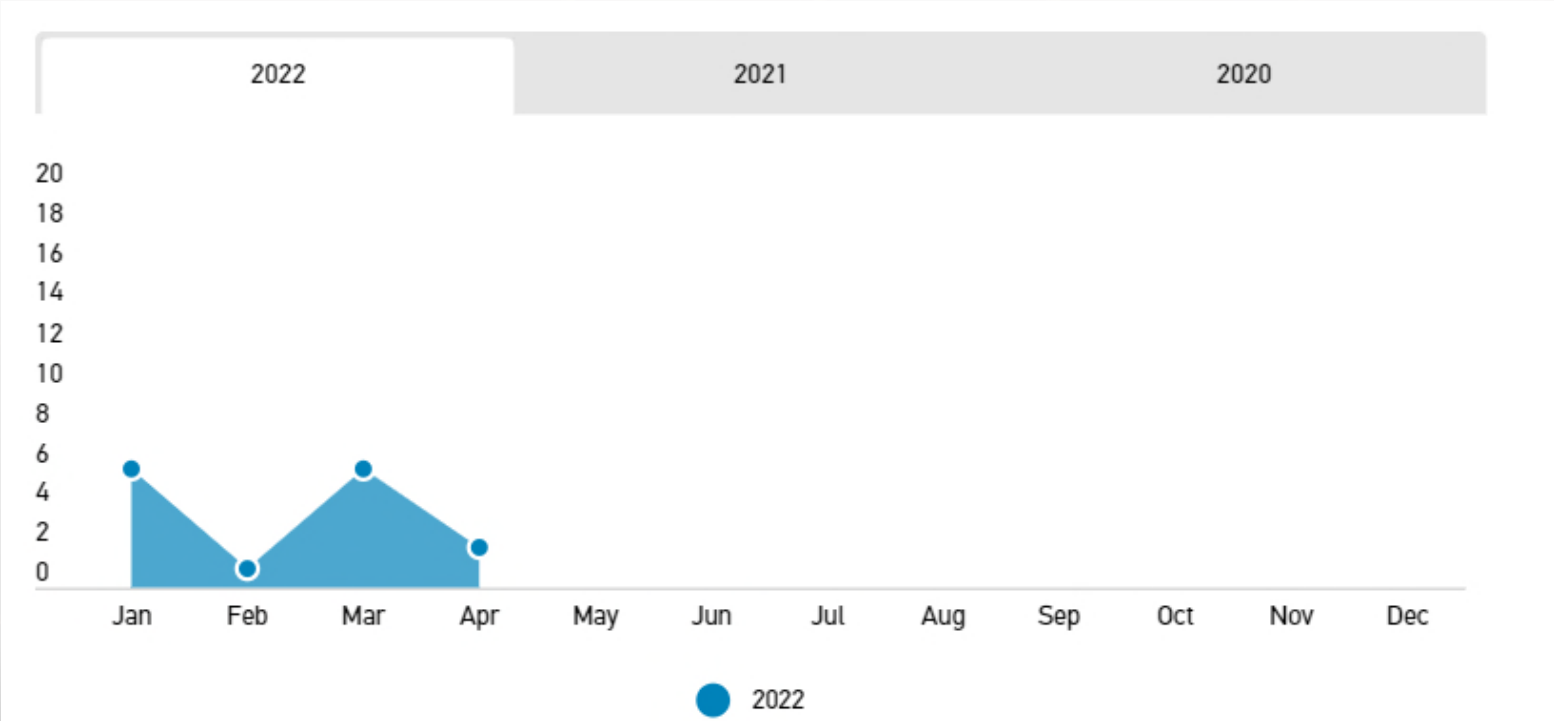
CCPA Litigation Trends 2021

Month Filed

The total number of filings in 2021 increased significantly from the previous year. There were 78 total filings in 2020 which jumped to 110 total filings in 2021, a 40% increase in the number of filings from year 1 to year 2 since the CCPA went into effect. Although still early since the CCPA's enactment, we are noticing a clear upward trend in the number of CCPA claim filings to date and anticipate this will continue.



CCPA Litigation Trends 2022

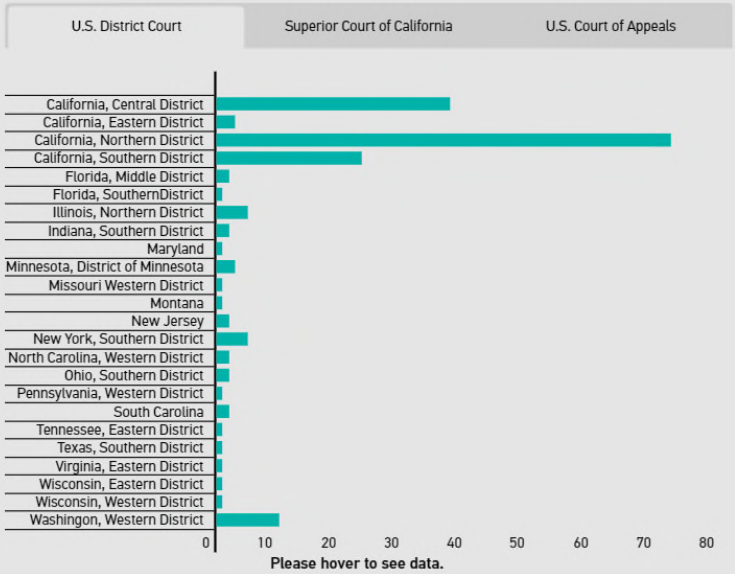


CCPA Litigation Trends *(cont'd)*

All the Buzz

Court

Most CCPA cases have been filed in the Northern District of California, followed by the Central District of California. This trend is consistent with privacy cases being a focal point of litigation around the country.

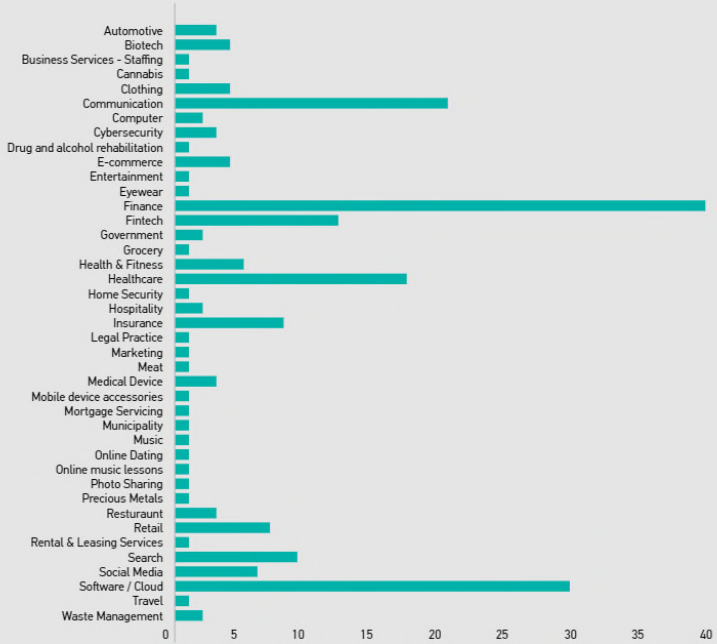


CCPA Litigation Trends *(cont'd)*

All the Buzz

Industry

Many of the CCPA cases focus on the technology sector with an emphasis on software. There has also been an increase in the number of cases impacting the financial industry and in turn, FinTech, followed by healthcare, search, and social media.



CCPA Litigation Trends *(cont'd)*

All the Buzz

Overview of Cases

- 230+ cases
- Vast majority are class actions
- Most cases are still pending, and none have been certified
- Pleading challenges pending

CCPA Litigation Trends *(cont'd)*

All the Buzz

Common Defense Theories

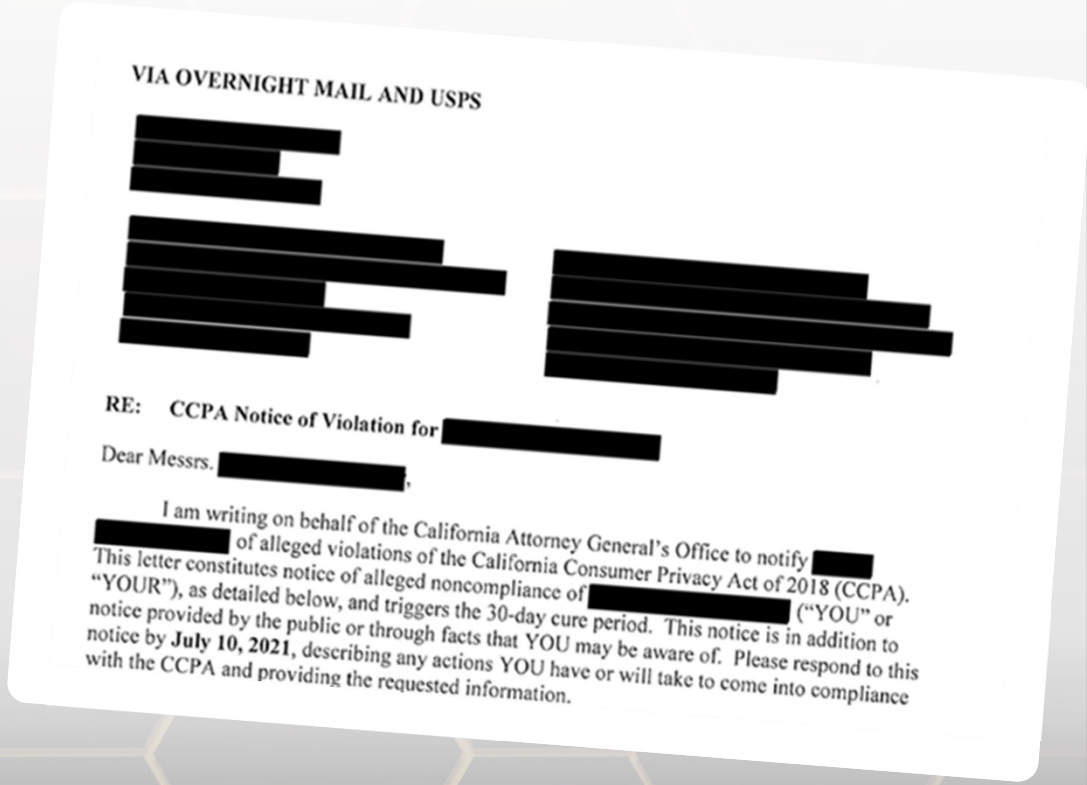
- Consumer data at issue does not qualify as "personal information" under the statutory definition
- Insufficient allegations to support a plausible inference that the defendant's security practices were unreasonable
- Insufficient allegations to support a plausible inference that data were "exfiltrated," as required by the statute
- CCPA expressly precludes UCL claims predicated on a CCPA violation
- Standing (resident, service provider)

All the Buzz

Lessons Learned: Mechanics of Enforcement Letters

Enforcement Letters:

- Addressed to CEO
- Deadlines: 30-day cure is immovable, flexibility with written response
- Time Constraints: Limited time to respond by the time it reaches outside counsel



VIA OVERNIGHT MAIL AND USPS

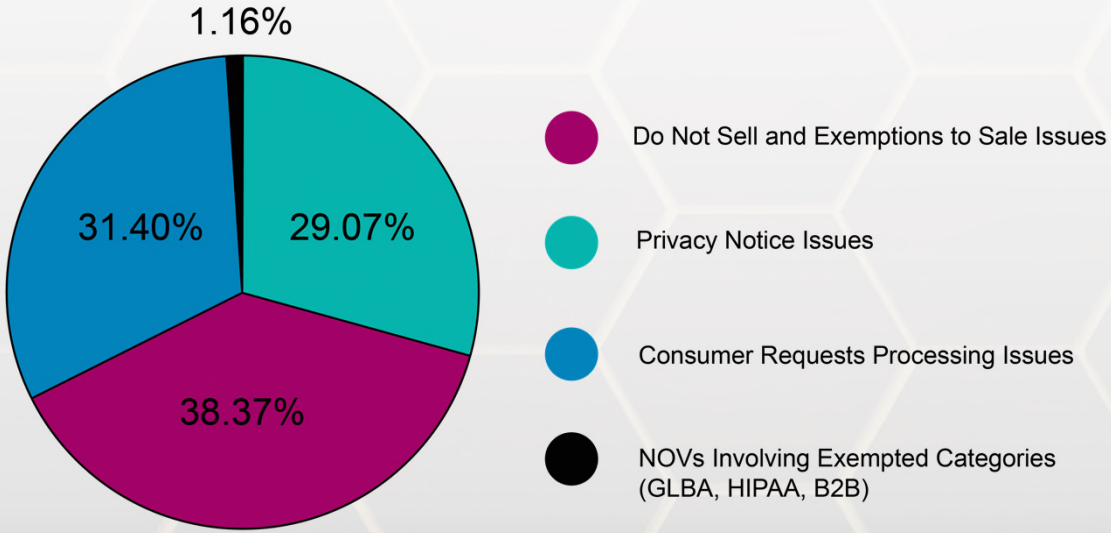
[redacted]

RE: CCPA Notice of Violation for [redacted]

Dear Messrs. [redacted],

I am writing on behalf of the California Attorney General's Office to notify [redacted] of alleged violations of the California Consumer Privacy Act of 2018 (CCPA). This letter constitutes notice of alleged noncompliance of [redacted] ("YOU" or "YOUR"), as detailed below, and triggers the 30-day cure period. This notice is in addition to notice provided by the public or through facts that YOU may be aware of. Please respond to this notice by **July 10, 2021**, describing any actions YOU have or will take to come into compliance with the CCPA and providing the requested information.

CCPA Enforcement Trends



All the Buzz

Comparison of Data Subject Rights

Right	Connecticut (CTDPA)	Utah (UCPA)	Colorado (CPA)	Virginia (VCDPA)	California (CPRA)	California (CCPA)
Access	✓	✓	✓	✓	✓	✓
Correct	✓	✓	✓	✓	✓	✗
Delete	Yes (data provided by or obtained about consumer*)	✓ (limited to data that consumer provided to controller)	✓ (personal data concerning consumer)	✓ (data provided by or obtained about consumer)	✓ (data collected from consumer)	✓ (data collected from consumer)
Private right of action	✗	✗	✗	✗	✓ (in the event of data breach)	✓ (in the event of data breach)
Opt-out of sale	✓	✓	✓	✓	✓	✓
Non-discrimination	✓	✓	✓	✓	✓	✓
Appeals process	✓	✗	✓	✓	✗	✗

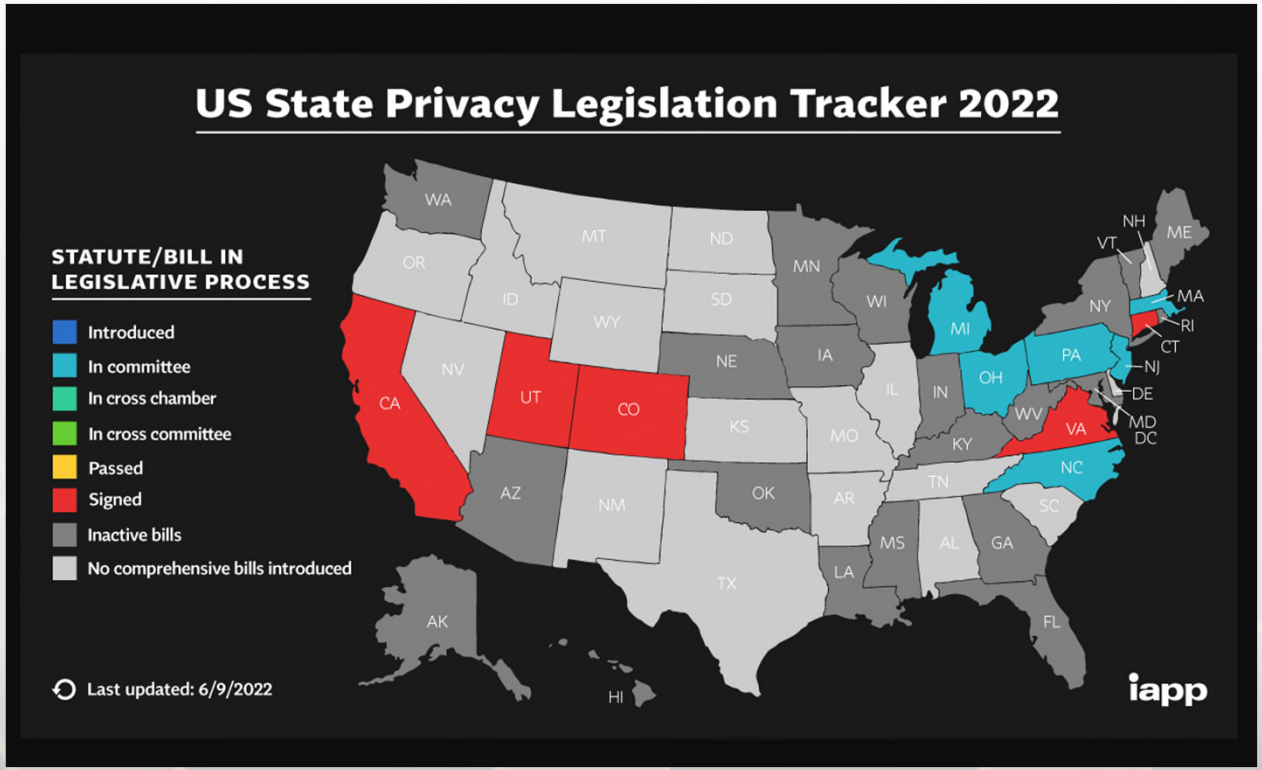
Other States With Privacy Laws

Effective Dates

Effective Date	CTDPA	UCPA	CPA	VCDPA	CPRA	CCPA
January 1, 2020						✓
January 1, 2023				✓	✓	
July 1, 2023	✓		✓			
December 31, 2023		✓				

Privacy Legislation in the US

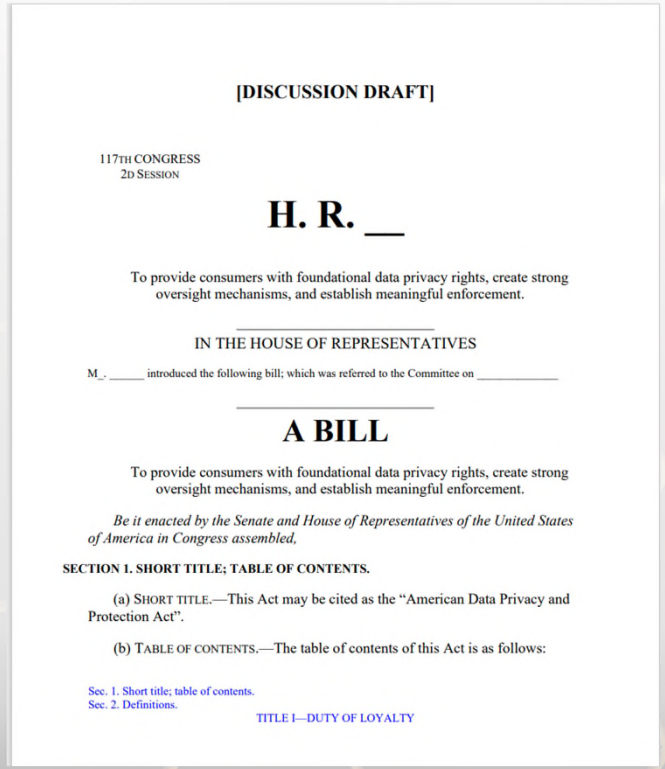
Source: https://iapp.org/resources/article/state-comparison-table/



Federal Privacy Law Update

MAYER | BROWN

Proposed American Data Privacy and Protection Act



[DISCUSSION DRAFT]

117TH CONGRESS
2D SESSION

H. R. __

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

IN THE HOUSE OF REPRESENTATIVES

M_. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

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 Data Privacy and Protection Act".

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

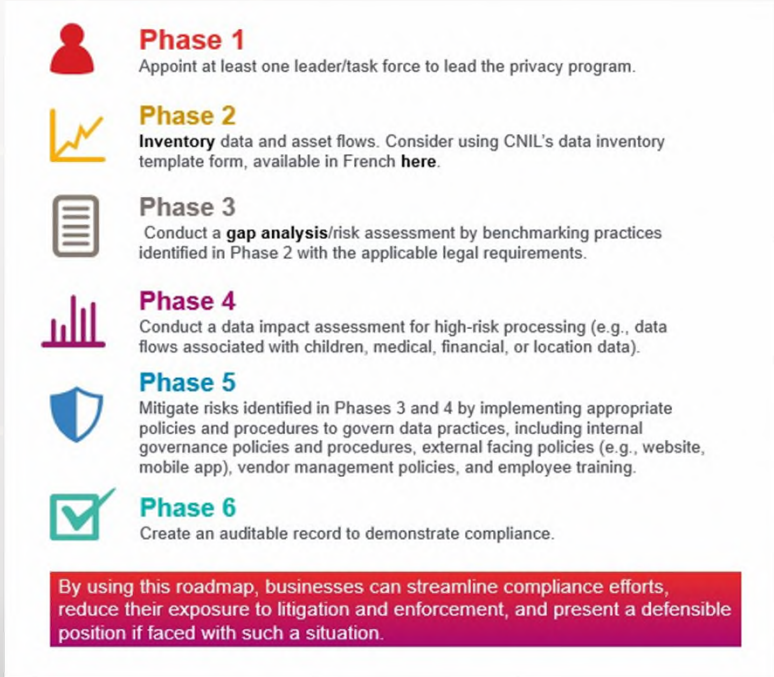
Preparing for the New Law(s): Privacy Compliance

MAYER | BROWN

Overview of Compliance

Six Phases

- Mayer Brown is experienced in guiding countless companies through these six phases and ultimately to privacy compliance



Privacy Tips for Deal Makers

MAYER | BROWN

Privacy Tips for Deal Makers

All the Buzz

Data Map

- Evaluate target company's information collect, use, and disclosure practices
- Identify data privacy and security laws applicable to target company and gaps in their compliance
- Evaluate risks based on types of personal data collected (e.g., health data, children's data, sensitive data)
- Review whether target company transfers data across borders and if they comply with applicable data localization laws

Privacy Tips for Deal Makers

Privacy Policy

- Review whether target company's public-facing privacy policy accurately describes its information collection, use, and disclosure practices
- Review whether target company is providing appropriate privacy notices to its job applicants, employees, and contractors
- Evaluate risk of liability based on target company's public and internal privacy policies

Privacy Tips for Deal Makers

Vendors

- Identify all vendors used by target company
- Evaluate whether target company properly vetted vendors for data privacy and security issues
- Review vendor contracts to ensure appropriate data privacy and security terms included
- Assess whether target company has entered into appropriate contracts with vendors if there is a cross-border data transfer

Privacy Tips for Deal Makers

Privacy Requests

- Evaluate target company's procedures and protocols for responding to data subject privacy requests, including:
  - Request to delete personal data
  - Request to access personal data
  - Request to correct personal data
  - Opt-out of sale of personal data
- Assess whether target company has failed to properly authenticate the identity of data subjects and/or not responded to prior requests

Privacy Tips for Deal Makers

Cybersecurity

- Assess whether target company has implemented appropriate security measures to safeguard data
- Review whether target company has adequate cybersecurity insurance for data breach coverage
- Evaluate if the target company has experienced data breaches in the past, how they responded to the past data breaches, and whether they provided appropriate notices to data subjects and/or enforcement authorities regarding the data breaches

Contractual Language Requirements

Contractual Language Requirements:

- GDPR
  - Determining Service Providers vs. Controller
- California Privacy Rights Act (CPRA) requirements
  - Determining whether company is a Service Provider, Contractor, or Third Party
- Other State Privacy Laws
  - Utah
  - Virginia
  - Colorado
  - Connecticut
  - Others?

Thank you and Questions

Dominique Shelton Leipzig
Partner, Los Angeles
+1 213 229 5152
dsheltonleipzig@mayerbrown.com

Scott Young
Partner, Salt Lake City
+1 801 907 2710
syoung@mayerbrown.com