MAYER | BROWN

A Legal Soap Opera: As the CCPA and CRPA Turn

Philip R. Recht
Partner
+1 213 229 9512
precht@mayerbrown.com

Lei Shen
Partner
1+ 312 701 8852
lshen@mayerbrown.com

Evan M. Wooten
Counsel
1+ 213 621 9450
ewooten@mayerbrown.com

September 17, 2020

Speakers

Philip R. Recht

Partner
+1 213 229 9512
precht@mayerbrown.com

The Managing Partner of Mayer Brown's Los Angeles office and co-leader of the firm's Public Policy, Regulatory & Political Law practice, Phil Recht represents clients in legislative, regulatory, enforcement and litigation matters before and involving federal, state, and local governments. He also handles grants, approvals, permits, and other government transactions. He has particular expertise in transportation, infrastructure, tribal gaming, health care, trade association, government contracts, and election law matters. *Legal 500* ranks Phil as a "Leading Lawyer" for Government Relations in the United States. He was named in 2019 to *The National Law Journal's* inaugural list of "Government Relations Trailblazers."

Lei Shen

Partner
+1 312 701 8852
lshen@mayerbrown.com

Lei Shen is a partner in the Cybersecurity & Data Privacy and Technology Transactions practices. Lei advises clients regarding a wide range of global data privacy and security issues. She advises companies on navigating and complying with state, federal, and international privacy regulations, including with regard to global data transfers, data breach notification, the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Children's Online Privacy Protection Act (COPPA), CAN-SPAM, and more. She also advises on e-commerce issues as well as on issues concerning mobile privacy and emerging technologies, such as telematics services, Internet of Things, and big data.

Evan M. Wooten

Counsel
+1 213 621 9450
ewooten@mayerbrown.com

Evan Wooten serves as Counsel in Mayer Brown's Los Angeles office, focusing on data privacy, disability law, and actions by public officials and government enforcement bodies. Evan is an experienced civil litigator and also assists clients in crafting contracts, policies, and terms of use to minimize litigation and government investigations. Evan also helps clients pursue legislative solutions in connection with state privacy law initiatives, such as the California Consumer Privacy Act (CCPA) and similar bills. Evan is a member of Mayer Brown's Cybersecurity and Data Privacy practice and one of Mayer Brown's lead disability law lawyers, counseling clients in ADA compliance and website accessibility, and defending disability lawsuits.

MAYER | BROWN

Agenda

- Overview of CCPA and Final CCPA Regulations
- CCPA Enforcement Actions and Class Action Lawsuits
- Journey to the CPRA
- Overview of CPRA and Key Differences between the CPRA and the CCPA
- Other Developments regarding CCPA-Like Laws


CCPA Overview
MAYER|BROWN

California Consumer Privacy Act (CCPA) - Overview

- **Became effective January 1, 2020, and became enforceable on July 1, 2020**
- Considered to be the **most sweeping privacy law in the U.S.**
- **Applies to for-profit companies doing business in California** that meet certain criteria
- Provides consumers with certain rights to their personal information, including:
  - The right to know what personal information is collected about them
  - The right to opt-out of the sale of their personal information
  - The right to delete certain of their personal information
  - The right to not be discriminated against for exercising their rights

MAYER | BROWN

Final CCPA Regulations

- California Office of Administrative Law (OAL) approved implementing Regulations on August 14, 2020, with immediate effect
- OAL made some changes to OAG's "final" Regulations, some of which were substantive:
  - Deletion of alternative language for opt-out link
  - Deletion of some sections in their entirety (e.g., Sections 999.305(a)(5), 999.306(b)(2) and 999.315(c))
  - Deletion of former Section 999.326(c) permitting business to deny requests from authorized agents that do not submit proof of authorization by consumer to act on their behalf

Requirements Under CCPA Regulations: Notices

- Notice at Collection requirements
  - What needs to be included in Notice at Collection
  - How to provide Notice at Collection
- Privacy Policy requirements
  - What needs to be included in Privacy Policy
  - How to provide Privacy Policy
- Other required notices
  - Notice of Right to Opt-Out and Notice of Financial Incentive

Requirements Under CCPA Regulations: Submission Methods and Responses

- Requirements for submission methods for Requests to Know and Requests to Delete
- Requirements for responding to Requests to Know and Requests to Delete
  - Timeframes
  - Requirements and restrictions on disclosures
  - Requirements for deletion
- Requirements for Requests to Opt-Out

Requirements Under CCPA Regulations: Other Requirements

- Training and record-keeping
- Verification of requests
  - Requirements concerning requests involving household information
- Authorized agents
- Consumers under the age of 16
- Right to Non-Discrimination requirements
  - What is considered a discriminatory practice
  - How to calculate the value of consumer data

CCPA Enforcement Actions

- Enforcement of CCPA began July 1, 2020
- OAG Enforcement Actions:
  - Initial letters sent to allegedly noncompliant businesses
    - Businesses identified based in part on consumer complaints using social media
    - Focused on missing privacy disclosures or "Do Not Sell" requirements

Class Action Lawsuits Under the CCPA

- Several class action lawsuits under CCPA already
- CCPA limits private right of action to breaches of certain sensitive personal data
  - Several traditional data breach claims under CCPA
- Despite this limitation, several class action lawsuits have focused on general violations of the CCPA, enforcement of which is reserved for the OAG
  - Lawsuits have focused on:
    - Violations of CCPA's notice provisions
    - Violations of opt-out requirements
    - Failure to implement reasonable security
    - Permitting leaks and unauthorized access

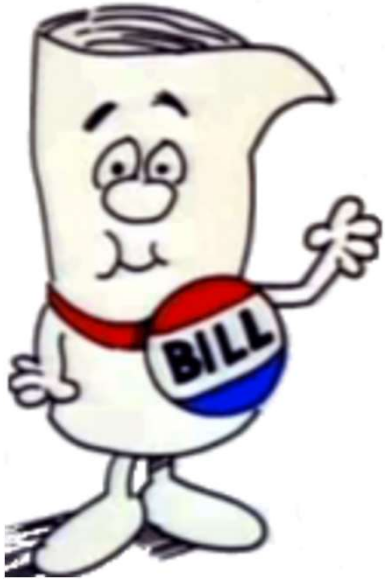
CPRA Journey

The Journey to the California Privacy Rights & Act of 2020 (CPRA) - Overview

- Prior to the CCPA, there were no "comprehensive" data privacy laws in the US
  - State and federal privacy laws were specific to:
    1. Conduct, *eg*, call recording (wiretap acts), telemarketing (TCPA), biometrics, etc.
    2. Industry, *eg*, health care (HIPAA), finance (GLBA), education (FERPA), etc.
- Otherwise, privacy governed by private contracts between business and consumers, often in the form of privacy policies or terms of use
- Stands in contrast to comprehensive regulations such as GDPR in EU

How the CCPA Became a Law

- In California, laws can be passed by voters as well as legislators
- In spring 2018, Californians for Consumer Privacy (CCP), led by NorCal businessman Alistair Mactaggart, qualified initiative 17-0039, the Consumer Right to Privacy Act
  - Broader definition of PI (*eg*, included psychometric data)
  - Fewer exemptions (*eg*, no GLBA exemption)
  - Expansive private right, whistleblower suits, and prosecution



From Ballot Initiative to Bill

- California Legislature rushed to convert initiative into a more balanced and workable bill
  - AB 375 finalized and signed into law on the deadline for CCP to withdraw (June 28, 2018)
  - SB 1121 enacted Sept. 23, 2018, to reorganize and correct drafting errors
- All parties anticipated bill would be further amended to address additional issues and additional stakeholders
  - Consumer rights advocates
  - Covered businesses
  - Regulators

Amending the CCPA

Some Fixes Passed:

- **AB 25**
  - B2B/employee exemptions
- **AB 874**
  - Limited fixes to PI, public data defs
- **AB 1146**
  - Vehicle data exemption
- **AB 1202**
  - Data broker registry established

Many Bills Failed:

- **AB 846**
  - Exempting loyalty programs from anti-discrimination
- **AB 873**
  - Additional fixes to PI definition
- **AB 1416**
  - Fraud prevention exemption
- **SB 675**
  - Expanded private right of action

Enter the CPRA

- On September 25, 2019, CCP files a new ballot initiative, originally titled the 'California Consumer Privacy Act of 2020' or CCPA 2020
- Initiative is amended 3 times (last on November 13, 2019) and retitled the 'California Privacy Rights Act of 2020' or CPRA, No. 19-0021
- Despite new title, CPRA does not replace CCPA: supersedes some provisions, leaves others intact, and adds new provisions

19 - 0021 Amdt. #

November 4, 2019

RECEIVED

NOV 13 2019

INITIATIVE COORDINATOR
ATTORNEY GENERAL'S OFFICE

Why the CPRA?

- CPRA's Findings and Declarations (§ D) state, 'the Legislature considered many bills in 2019 … some of which would have significantly weakened [the CCPA]'
- CPRA proposed to ensure consumer rights are 'strengthened' rather than 'diluted' (§ E)
- Purposes for CPRA:
  1. Avoid perennial legislative fights over new amendments
  2. Address constitutional flaws
  3. Equivalence/adequacy

From Bill Back to Ballot

- CPRA needed 685,534 valid signatures
- CCP submitted 930,942 signatures, requiring 74% validity
- Signature collection impeded by shelter in place orders, submitted at eleventh hour, causing Secretary of State to submit to counties for certification a day late
- Mactaggart sued Secretary of State to ensure that signatures would be verified prior to June 25, 2020
- Court granted writ relief and the CPRA qualified for November ballot on June 24, 2020

"Proposition 24"

Proposition 24

July 3, 2020
Initiative 19-0021 (Amdt. #1)

BALLOT LABEL

AMENDS CONSUMER PRIVACY LAWS. INITIATIVE STATUTE. Permits consumers to: prevent businesses from sharing personal information, correct inaccurate personal information, and limit businesses' use of "sensitive personal information," including precise geolocation, race, ethnicity, and health information. Establishes California Privacy Protection Agency. Fiscal Impact: Increased annual state costs of at least $10 million, but unlikely exceeding low tens of millions of dollars, to enforce expanded consumer privacy laws. Some costs would be offset by penalties for violating these laws.

Support and Opposition

Support

- Consumers
  - Polling at 81%
- Common Sense Media
- Consumer Watchdog
- (Andrew Yang)

Neutral

- Cal Democratic Party
- Consumer Reports
- Cal Labor Federation
- Electronic Frontier Foundation
- Cal Chamber

Oppose

- Consumer Fed of California
- ACLU of California
- ANA and other advertising trades
- Cal. Nurses Assoc.
- (Mary Stone Ross)


CPRA

Key Differences Between the CPRA and CCPA

- New consumer rights and protections
  - Creates new category of "sensitive personal information (PI)"
  - Includes PI revealing SSN, driver's license, state ID or passport number; financial account access info; precise geolocation; race, ethnicity, religious or philosophic beliefs, or union membership; private mail, email, or text messages; genetic data; data re health, sex life, or sexual orientation
  - Requires businesses to provide separate disclosure of categories of sensitive PI collected and uses to which put
  - Provides consumers right to limit use and disclosure of such PI to functions necessary to business purpose for which it was collected
  - Requires business to provide new "Limit the use of my sensitive PI" link (can be combined with "Do not sell or share" link)

Right to Correct Inaccurate Data

- Allows consumers to request correction of inaccurate PI possessed by businesses
- Request to correct must be made through verifiable consumer request
- Nature of correction rights and obligations - including business' duty to investigate accuracy of requested correction and right to reject questionable requests, consumer right to provide written response to rejected requests - to be determined in new regulations

Enhanced Data Protection, Opt Out, Deletion and Resale Limitation Rights

- **Buyer use promises:** Requires business that sells PI to require buyer to contractually promise to use PI only for specified purposes, notify seller of subsequent sale or disclosure of PI, allow seller to enforce promises
- **Downstream deletions:** Requires business receiving deletion request to notify contractors, service providers, and third parties to which PI was sold or provided to delete PI unless impossible or involves disproportionate effort
- **Shared PI:** Requires business to disclose categories and purposes of PI "shared," with or without consideration, for "cross-context behavioral [i.e., third party] advertising" purposes; expands opt out to prohibit such sharing; opt out link to now read "Do not sell or share my [PI]"
- **Automatic opt outs:** Requires business to allow consumers to use automatic signal from platform, browser, or device setting to opt out or limit use of sensitive PI (as opposed to links re same)

Other Enhanced Rights

- **Profiling:** Requires business to disclose "profiling" activities (i.e., automated processing of PI to predict consumer preferences, interests, behavior, work performance, etc.) in response to consumer access requests and allow opt out of same
  - Details to be determined in rulemaking
- **Look-back duration:** Allows consumers to request and access PI collected by businesses beyond the current 12 month look-back limit
  - Applicable to PI collected after January 1, 2022
  - Details, including circumstances under which businesses can refuse, to be determined in rulemaking

Tighter Restrictions on Data Collection, Use and Storage of PI

- **Use limitation:** Prohibits business from collecting additional categories of PI or using PI for new, undisclosed purposes unless consumer given prior notice
- **Data minimization:** Requires business to minimize collection, use, retention, and sharing of PI to that reasonably necessary to achieve disclosed purposes of same
  - Business must inform consumers of duration of retention at or before collection

Clarifies and Expands "at Or Before Collection" Notice Requirements

- Allows business without direct consumer relationships to provide such notice on internet homepage
- Requires business collecting PI from consumers on premises or in vehicle (e.g., through cameras, Wi-Fi sniffers) to provide clear and conspicuous notice at such location

New Benefits to Business

- Expands "publicly available information" PI exemption to include information made available to general public by the consumer, by a person to whom the consumer has disclosed the information without restricting it to a specific audience (e.g., public Facebook page), or from widely distributed media (e.g., newspaper)
- Retains existing CCPA exemption for government records data
- Exemptions apply to sensitive PI

Other Benefits to Business

- Extends employee and B2B data exemptions to January 1, 2023
  - California legislature assumedly will attempt to develop permanent solution in interim
- Doubles from 50,000 to 100,000 the number of consumers whose PI a small business must annually buy or sell to qualify as a covered business

Creation of New Enforcement Agency

- Creates new California Privacy Protection Agency with responsibility to administer, implement, and enforce CPRA
- Transfers responsibility from AG's office to new agency on earlier of July 1, 2021 or 6 months after new agency indicates it is ready for the transfer
- Provides initial government loan funding of $10 million/year, to be repaid as fines and settlement funds collected by the agency allow
  - 91% of collected funds to be invested with earnings going to general fund; 9% available for grants to nonprofit privacy organizations, law enforcement, schools
  - May create pressure for heightened enforcement efforts

New Enforcement/Penalty Rules

- For CCPA/CPRA violations enforced by new agency, eliminates automatic 30-day cure right; instead provides agency discretion to allow cure or not file complaint based on good faith factors (e.g., lack of intent to violate, voluntary effort to cure before agency complaint)
- Triples administrative fines and civil penalties—from $2500 to $7500—for violations involving minors
- For data breaches subject to private right of action (PRA), provides that adoption of reasonable security measures after breach does not constitute a cure
  - Expands PRA to include breaches involving consumer login credentials (i.e., email address plus password or security Q&A)

CPRA Interpretations and Amendments

- Requires new agency to issue regulations interpreting various new and amended provisions added by CPRA by July 1, 2022
- Allows legislature to amend CPRA by majority vote, but only if consistent with and furthers the purpose and intent of the CPRA

Timing Issues

- If approved by voters on November 3, 2020, CPRA becomes "effective" five (5) days after vote count is certified by Secretary of State (probably early December 2020)
- CPRA not "operative" until January 1, 2023, and then only applies to PI collected on or after January 1, 2022
- No CPRA enforcement allowed until July 1, 2023, and then only for violations occurring on or after that date
  - Creates 6 month grace period, akin to CCPA scheme
- Until CPRA is both operative and enforceable, CCPA (including provisions amended by CPRA) to remain in full force and effect (i.e., enforceable)

Other Developments

Other Developments – Other States Proposing CCPA-like Laws

- In recent years, privacy laws have been introduced in at least 26 states
  - Some bills comprehensive like CCPA, others narrowly focused (e.g., applicable only to internet service providers, dealing with data security only)
  - For comprehensive bills, issues of greatest controversy have been opt out vs. opt in, extent of PRA
- Proposals in 6 states (CT, HI, LA, MA, ND, TX) set aside by legislature in favour of study or task force on topic
- Proposals in others—most conspicuously WA—defeated over inclusion of PRA
- As of July 2020, proposals actively pending in only 10 states
  - Given COVID-shortened legislative sessions and potential for CPRA passage, prospects for near-term state enactments unclear

Other Developments—ULC Model State Law

- Uniform Law Commission (ULC)
  - Given lack of state enactments and absence of other model state law efforts, ULC began model law effort in 2019
  - Current draft follows CCPA "individual rights" approach, but draws from GDPR (e.g. data minimization), CPRA (e.g., broad publicly available data exemption), other laws and proposals
  - Much more skeletal than CCPA, with significant leeway for state Attorneys General to fill in details through rulemakings
    - AGs encouraged to seek uniformity among states; also to give deference to voluntary industry consensus standards
  - Currently has limited PRA—most contentious topic
  - Final version to be submitted for approval July 2021
  - If approved, could be influential

Federal Activity

- Various proposals introduced in Congress in recent years by both Democrats and Republicans
- Generally follow the CCPA framework
- Differ as to entities covered, extent of data access by consumers
- Biggest differences are whether bills (1) pre-empt all state laws or only those less restrictive, and (2) include PRA
- Given current Congressional gridlock, no near-term prospect of passage
- Election results could make a difference, but doubtfully high priority item for either Biden or Trump administration

Tech Reconnect 2020 – Upcoming Programs

- September 22 Tech Talks Podcast: New Rule for Online Platforms and Search Engines Offering Services to Businesses in the EU and UK

- September 29 Tech Talks Podcast: Artificial Intelligence Licensing: What You Need to Know
- Watch the Tech Reconnect Calendar link located in the resource widget for updates, registration and content. October programming to be announced soon!

Disclaimer

- These materials are provided by Mayer Brown and reflect information as of the date of presentation.
- The contents are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.
- You may not copy or modify the materials or use them for any purpose without our express prior written permission.

Americas | Asia | Europe | Middle East

mayerbrown.com