MAYER | BROWN

CCPA Fundamentals

What you need to know and do now for the California Consumer Privacy Act

Stephanie Duchene
Partner
+1 213 229 5176
sduchene@mayerbrown.com

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

Kendall Burman
Counsel
+1 202 263 3210
kburman@mayerbrown.com

June 26, 2019

Speakers

Stephanie Duchene, Partner – Los Angeles

Stephanie Duchene is a partner in Mayer Brown's Los Angeles office and a member of the Insurance group. She focuses her practice on representing insurance companies, producers and other insurance licensees and insurance-related service providers in complex and sensitive regulatory matters, including negotiating and resolving significant single and multistate examinations and investigations, counseling clients on compliance with licensing, claims handling, marketing and advertising rules, and advising clients on the development of new insurance products from initial concept through regulatory approval and into the market. She advises clients on all lines of insurance, including accident, life and health, property and casualty, as well as surplus and excess lines. Additionally, she regularly counsels insurtech companies, traditional carriers and non-insurance entities on the intersection of insurance law and innovation in the industry.

Lei Shen, Partner – Chicago

Lei Shen is a partner in the Cybersecurity & Data Privacy and Technology Transactions practices in Mayer Brown's Chicago office. 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, such as electronic contracting and signatures, and on issues concerning mobile privacy and emerging technologies, such as telematics services, Internet of Things, and big data.

Kendall Burman, Counsel – Washington DC

Kendall Burman is a Cybersecurity & Data Privacy counsel in Mayer Brown's Washington DC office. Kendall advises a broad range of clients, including financial services and technology companies, on legal, regulatory, and policy issues involving emerging technologies, security, privacy, and the flow of information across borders. Her practice focuses on advising clients on their privacy and data security policies and practices, including advising companies on how to develop their information programs in ways that comply with the law and industry best practices. Kendall also advises and advocates for clients on new and complex policy and compliance issues involving big data, artificial intelligence, and other technologies.

Agenda

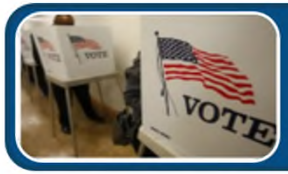
1. How'd we get here?
2. Who and what does the CCPA apply to?
3. What does the CCPA require?
4. Exemptions and Enforcement
5. Tips for early-stage readiness
6. Further changes on the horizon

How'd we get here?

The origin story behind the CCPA

MAYER | BROWN

California Consumer Privacy Act (CCPA): How We Got Here



1972 California Constitution amended to include the right of privacy as an "inalienable" right

Between 1972 and 2018 California adopted numerous privacy laws, including Online Privacy Protection Act, Privacy Rights for California Minors in the Digital World Act, Shine the Light, and Data Breach Law

Cambridge Analytica

In March 2018 the Cambridge Analytica scandal highlighted potential privacy abuses domestically and abroad

In May 2018 California for Consumer Privacy announced it had obtained sufficient signatures to place the California Consumer Privacy Act on the November 2018 ballot

CCPA – Procedural Posture

Passed, signed on 6/28/18 as a compromise between activists and industry

Legislature began amending almost immediately; legislative activity continues

AG held public forums earlier in the year and we await the regulations

CCPA—Overview

- Signed into law on June 28, 2018
- Effective on January 1, 2020
- Considered to be the most sweeping privacy law in US
- Final content of bill remains in flux
- Multiple significant amendments gaining traction
- Awaiting AG regulations/guidance

Key Definitions

Business

Consumer

Personal Information (PI)

Who and what does the CCPA apply to?

Focus on CCPA definitions

MAYER | BROWN

Who Does the CCPA Apply to?

Applies to “businesses” that collect (or determine the purposes and means of processing) “consumer” “personal information”

CCPA—Definitions and Scope

Business Definition #1

- Any sole proprietorship, partnership, LLC, corporation, association or "other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that:
- Collects consumer PI or determines the "purposes and means of the processing of" PI either alone or jointly with others
- Conducts business in California
- Satisfies one of the following thresholds:
  - Gross revenue threshold: gross revenues in excess of $25 million USD, as adjusted (Civ. Code § 1798.140(c)(1)(A))
  - Collection threshold: buys, receives, sells or shares PI of 50,000 or more consumers, households or devices (Civ. Code § 1798.140(c)(1)(B))
  - Sale threshold: derives 50 percent or more of its annual revenues from "selling" consumer personal information (Civ. Code § 1798.140(c)(1)(A))

CCPA—Definitions and Scope

Business Definition #2

- Any entity that controls or is controlled by a business as defined in definition #1 and that "shares common branding with the business" (Civ. Code § 1798.140(c)(2))
  - "Control" or "controlled" means:
    - "Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business"
    - "Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions"
    - "Power to exercise a controlling influence over the management of a company"
  - "Common branding" means a "shared name, service mark, or trademark"

CCPA—Definitions and Scope

Consumer Definition

- Natural person who is a California resident (as defined in Section 17014 of Title 18 of California Code of Regulations)
- Much broader than definition of consumer under other privacy laws which typically require a transactional nexus (e.g., includes employees)
- Definition being challenged during lobbying process, likely employee component will be removed

CCPA—Definitions and Scope

Personal Information Definition

- Information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" (Civ. Code § 1798.140(o)(1))
- Does not include publicly available information made available from government records (Civ. Code § 1798.140(o)(2))
- Expansive definition – far broader than prior privacy laws
- Subject of legislative amendments

CCPA—Definitions and Scope

Personal Information Definition

- Includes but is not limited to the following if it identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household:
  - **Identifiers**: real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, Social Security number, driver's license number, passport number, or similar
  - Any category of PI described in Civ. Code § 1798.80(e)
  - Characteristics of protected classifications under California or federal law
  - **Commercial information**, including records of personal property, products or services purchased, obtained or considered or other purchasing or consuming histories or tendencies
  - **Biometric** information
  - **Internet or other electronic-network activity information**, including but not limited to browsing history, search history and information regarding a consumer's interaction with a website, application or online advertisement
  - **Geolocation** data
  - Audio, electronic, visual, thermal, olfactory or similar information
  - Professional or employment-related information
  - **Education information**, defined as information that is not publicly available personally identifiable information as defined in Family Educational Rights and Privacy Act (Civ. Code § 1798.140(o)(1)(A)-(K))
  - **Inferences** drawn from any information identified in this subdivision to create a profile about a consumer reflecting preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes

What does the CCPA require?

Recognizing individual rights in consumer personal data

MAYER | BROWN

CCPA Creates Significant New Privacy Rights and Corresponding Business Obligations

Consumer Rights	Business Obligations
Right to Know Right to request categories and specific pieces of personal information collected by business in past 12 months.	• Make available two or more designated methods for submitting consumer request for PI (Civ. Code § 1798.130(1)) • Disclose and deliver PI "free of charge" within 45 days of "receiving verifiable consumer request" looking back 12 months; business entitled to "promptly" take steps to determine whether request is verifiable consumer request (Civ. Code § 1798.130(2))
Right to know business's data practices.	• At or before point of collection of PI, inform consumers about categories collected and purposes for use (Civ. Code § 1798.100(b))
Right to know rights under the CCPA.	• Must be disclosed on online privacy policy, California-specific description of consumer privacy rights, or website – List of categories of PI collected, sold or disclosed for business purposes about consumers in preceding 12 months by reference to enumerated categories listed in CCPA that most "closely describe" (Civ. Code § 1798.130(a)(5)(B)-(C)) – Description of consumer's rights under the CCPA, including right to know, right to deletion, right to opt out and methods for submitting requests (Civ. Code § 1798.130(a)(5)(A))

CCPA Creates Significant New Privacy Rights and Corresponding Business Obligations

Consumer Rights	Business Obligations
Right to Opt Out Right to opt out of sale of personal information	• Must provide "clear and conspicuous link" on homepage titled "Do Not Sell My Personal Information" that directs to opt-out website without additional account (Civ. Code § 1798.135(a)(1)) • Must include description of right to opt out along with separate link to "Do Not Sell My Personal Information" page in privacy policy/California rights page (Civ. Code § 1798.130(a)(2)(A)-(B)) • Must ensure all individuals responsible for handling consumer inquiries about business's privacy practices or compliance with the CCPA are informed of consumer's right to opt out and how to direct consumers to exercise right • Must respect the decision to opt out for at least 12 months before requesting authorization of sale • "Sell" includes "releasing, disclosing, transferring, or otherwise communicating" a consumer's PI to another business or third party "for monetary or other valuable consideration" (Civ. Code 1789.140(t)(1)) • A sale does not occur when: – Business transfers PI to a third party as an asset that is part of a transaction in which the third party assumes control of all or part of the business (Civ. Code §1798.140(t)(2)(D)) – When PI is disclosed to a "service provider" (Civ. Code §1798.140(t)(2)(C))

CCPA Creates Significant New Privacy Rights and Corresponding Business Obligations

Consumer Rights	Business Obligations
Right to Delete Right to compel business to delete PI that has been collected	• Must delete consumer's PI from records and direct any service providers to delete the consumer's PI from their records (Civ. Code § 1798.105(d)) • Numerous Exceptions – not required to delete PI if needed to: – Complete the transaction for which the PI was collected – Comply with a legal obligation – Enable solely internal uses that are reasonably assigned with the expectations of the consumer based on the consumer/business relationship – Otherwise use the PI internally in a lawful manner that is compatible with the context in which the consumer provided the information
Antidiscrimination Unclear prohibition against discriminating based on exercise of any CCPA rights	• Cannot discriminate against consumer because consumer exercises CCPA rights, such as: – Denying goods or services to consumer – Charging different prices or rates for goods or services, including through use of discounts or other benefits or imposing penalties – Providing a different level of goods or services to consumer – Suggesting that consumer will receive different price, rate or quality for goods or services

Who is exempt and how is CCPA enforced?

No simple answers

MAYER | BROWN

Is Anyone Exempt From the CCPA?

- CCPA contains exemptions for personal information collected, processed or disclosed pursuant to GLBA, and under FCRA, HIPAA and certain other laws
  - Exemptions generally limited and apply only to personal information covered by those statutes, so financial institutions need to comply with CCPA with respect to other information collected
- New amendment, AB 981, if passed, exempts insurance institutions, agents and support organizations from CCPA, but imposes CCPA-like requirements

GLBA Exemption

- GLBA covers nonpublic personal information (NPI) of consumers and customers of financial institutions
  - Customers and consumers are natural persons who establish customer relationship (e.g., obtain financial product or service) or provide NPI to determine eligibility for financial product or service
  - NPI includes personally identifiable financial information (e.g., information provided to obtain financial product or service or resulting from transaction involving product or service or information obtained about consumer) and lists of persons that are derived from nonpublic information (e.g., customer lists)
- GLBA requires financial institutions to:
  - Provide initial and annual written notices summarizing information collection, use and dissemination practices
  - Provide customers with opportunity to opt out of having "nonpublic personal information" disclosed to unaffiliated third parties (except as otherwise permitted by exceptions)
  - Adopt policies and procedures to maintain security, confidentiality and integrity of customer records and data

GLBA Exemption

- CCPA exemption regarding the GLBA provides:
  - CCPA shall not apply to personal information collected, processed, sold or disclosed pursuant to the GLBA and implementing regulations (Civ. Code 1798.145(e))
  - Exemption does not apply to Section 1798.150 (CCPA's private right of action for unauthorized access/data breaches)
- Exemption is limited – applies only to information collected pursuant to the GLBA, which is a limited subset of information – other information still subject to CCPA

New Amendments Exempting Insurance – AB 981

- Amends California Insurance Code section 791.01 et seq. (the Insurance Information and Privacy Protection Act – IIPPA)
- Exempt insurance companies, agents and support organizations that are subject to the IIPPA, except:
  - For the limited private right of action for data breaches; or
  - For any business activity not subject to IIPPA
- The Insurance Information and Privacy Protection Act (IIPPA) is a long-standing privacy law applicable to insurance companies, agents and insurance support organizations that establishes privacy standards for collection, use and disclosure of information gathered in connection with insurance transactions

New Amendments Exempting Insurance – AB 981

- Unlike other CCPA exemptions, which are based on type of information at issue, this exempts insurance entities as a whole
- However, it incorporates specific CCPA concepts into the IIPPA:
  - Mirroring CCPA definitions for personal information,
  - Granting a limited "right to know," "right to opt out" and "right to delete,"
  - Requiring insurers to provide certain disclosures and privacy notices.
- Seeks to retain the California Insurance Commissioner as the single enforcer/regulator for any privacy-related violations by insurers

Getting prepared

Tips for early-stage readiness

MAYER | BROWN

CCPA Compliance Failures Could Be Costly

- California AG can seek statutory damages for violations of the CCPA that are not cured within 30 days
  - Up to $7,500 per intentional violation, $2,500 per unintentional violation
- Consumers whose "nonencrypted or nonredacted personal information… is subject to an unauthorized access and exfiltration, theft, or disclosure" have limited private right of action against violators
  - Can recover between $100 to $750 per incident or actual damages, whichever is greater
  - Need not prove actual damages to qualify for statutory damages
  - May seek injunctive or declaratory relief
  - This right only attaches to compromise of data already protected under CA data-breach notification statute
- Large-scale breaches that result in CCPA violations could thus impose significant penalties on organizations in addition to the standard expenses associated with breaches

Companies May Draw On GDPR-Compliance Work

- Even though coverage and requirements of GDPR and CCPA differ in many respects, they share many common types of obligations that organizations will need to address:
  - Identify necessary changes to address new individual rights
  - Update privacy notices and internal privacy policies
  - Review internal processes
  - Update recordkeeping
  - Update vendor agreements
  - Review security measures
  - Review data breach response plan

Deep Dive – Can Data Be De-identified?

- "De-identified" information may not be covered by the CCPA, so businesses may wish to consider whether they can de-identify some of the personal data they collect
- CCPA (as amended) defines "de-identified" data to mean information that does not identify, or is not reasonably linkable to a particular consumer. Requires the business to:
  - Take reasonable measures to ensure the data is not re-identified
  - Make no attempt to re-identify the information
- What data could be subject to de-identification? Would de-identified data still be valuable or useful? Are there some data elements that cannot be de-identified consistent with other business goals?

CCPA "Early-Stage" Readiness Steps

- **Perform Data Classification/Mapping for CCPA Expanded Definition of Personal Information**
  - Survey systems and processes considering the CCPA's expanded definition of what information is considered "personal" to determine what information is collected, how it is used and what may or may not be subject to exemption
- **Update Privacy Policies and Notices**
  - The CCPA requires transparency regarding the rights conferred under it and about the categories of personal information collected and how they are used

CCPA "Early-Stage" Readiness Steps

- **Determine whether you are selling (or disclosing "for money or other valuable consideration") personal information, and, if so, build opt in/opt out functions and procedures**
  - The CCPA allows consumers to opt out of the sale of their personal information
  - Need to provide a function on website to allow for this and develop procedures for handling opt-out requests

CCPA "Early-Stage" Readiness Steps

- **Identify Third Parties and Update/Supplement Contracts**
  - The CCPA allows businesses to share personal information with service providers (a defined term) without it being considered a sale (from which a consumer could opt out)
  - To qualify as a service provider the written agreement between the parties must contain certain provisions
  - Analyze the data flow in their third-party relationships and amend written agreements accordingly

CCPA "Early-Stage" Readiness Steps

- **Evaluate Data Security/Review Incident Response Plan**
  - The CCPA includes a private right of action in the event of a data breach
  - Proposed amendments are likely to amend the private right of action
  - Revisit incident response plan to ensure it emphasizes rapid detection, containment and mitigation

CCPA "Early-Stage" Readiness Steps

- **Develop Policies and Procedures for Governance Program**
  - The new information rights will necessitate new, or changes to existing, internal privacy programs
  - Consider designating a role with responsibility for CCPA compliance and oversight
  - Have processes in place to receive and track consumer requests regarding personal information
  - Consider workforce training, particularly for workers that will be handling individual requests

Moving target

Further changes on the horizon

MAYER | BROWN

Multiple CCPA Amendments Pending

- Many subject businesses currently advocating for variety of clarifications and changes to law's interpretation or implementing regulations to ease compliance burdens
- Multiple amendments submitted to alter CCPA's substantive requirements:
  - Modifying definition of "consumer" to exclude employment-related information (AB 25)
  - Clarifying that businesses may continue to offer "customer loyalty programs" (AB 846)
  - Amend definition of "de-identified" data and remove household from the PI definition (AB 873)
  - Exclude "publicly available information" from the definition of "personal information" and clarify it does not include de-identified or aggregated consumer information (AB 874)

CCPA Amendments

- Exempting insurance organizations subject to the Insurance Information and Privacy Protection Act, but incorporating CCPA-like requirements into the insurance code (AB 981)
- Create registry for data brokers with the California Attorney General (AB 1202)
- Eliminate need for businesses to provide toll-free telephone numbers for consumers to submit data requests (AB 1564)
- Exempt disclosure of PI to government agencies and to third parties for purposes of detecting security incidents or preventing fraudulent or illegal acts (AB 1416)
- Proposed amendment to expanding private right of action to allow consumers to sue for violations of act besides certain data breaches supported by AG, but effectively dead (SB 561)

CCPA—Regulations, Enforcement, Private Right of Action

AG Regulatory Obligations

- AG must "solicit broad public participation and adopt regulations" on or before July 1, 2020 (Civ. Code §1798.185(a)). Public hearings have occurred this year.
- Regulations must address certain topics, including:
  - Update categories of PI and definition of unique identifiers to address "changes in technology, data collection practices, obstacles to implementation, and privacy concerns"
  - Update designated methods to submit requests to obtain PI
  - Establish any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights
  - Establish rules and procedures to "facilitate consumer's ability to obtain information with goal of minimizing administrative burden on consumers, including rules on verifiable request." (Civ. Code §1798.185(a)(7))

State-Level Policy Also Continues to Evolve

- New comprehensive consumer privacy obligation in Nevada
- A number of states have introduced comprehensive data-protection legislation (HI, IL, MD, MA, MS, NV, NJ, NM, NY, ND, PA, RI, WA)
- Some legislation mimic requirements of CCPA, others take different approach to data privacy
- Creates risk of patchwork of data-privacy requirements across states

Americas | Asia | Europe | Middle East

mayerbrown.com