



MINTZ

California Consumer Privacy Act: Overview

February 6, 2019



SPEAKERS



Cynthia J. Larose

Chair, Privacy & Cybersecurity Practice

Boston, MA

CJLarose@mintz.com // +1.617.348.1732

- Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E)
- Represents companies in information, communications, and technology, including e-commerce and other electronic transactions
- Counsels clients through all stages of the "corporate lifecycle," from start-ups, through mid- and later-stage financings, to IPO, and has broad experience in technology and business law, including online contracting issues, licensing, domain name issues, software development, and complex outsourcing transactions



Brian H. Lam

Attorney, Privacy & Cybersecurity Practice

San Diego, CA

BHLam@mintz.com // +1.858.314.1583

- Designated a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals, and is also a Certified Information Privacy Professional (CIPP-US), Certified Information Privacy Manager (CIPM), and a Certified Information Systems Security Professional (CISSP)
- Focuses practice on providing practical advice that enables companies to pursue their business in a competitive environment while reducing risk associated with the collection, use, storage, transfer, and potential loss of data
- Member of California Cybersecurity Task Force

HOUSEKEEPING NOTES FOR AUDIENCE

- The webinar will be recorded.
 - The recording and slides will be sent to all participants after the webinar.
- If you cannot hear the presentation, please go to the “Event Info” tab and click “Connect to Audio”.
- If you are calling in through your computer, please be sure to turn up the computer's volume.
- Questions will be answered after the presentation in the interest of time.
 - Use the Q&A application to submit a question.
- The code required for CLE credit will be announced at a random point during the presentation.

Covered in this Presentation

CCPA Enforcement Date and Rulemaking Activity

Overview of CCPA

CCPA Obligations by Entity Type

CCPA Consumer Rights

Enforcement of CCPA

CCPA Compliance Strategies

CCPA Enforcement Date and Rulemaking Activity



CCPA Timeline and Enforcement Date

2016	<ul style="list-style-type: none">• Real Estate Developer Alastair Mactaggart teams up with others to draft a proposed California privacy initiative.
2017	<ul style="list-style-type: none">• Initiative submitted; signature gathering begins.
May 2018	<ul style="list-style-type: none">• Over 600,000 signatures collected.
June 22, 2018	<ul style="list-style-type: none">• California Legislature offers to pass sweeping privacy act if Mactaggart pulls his initiative; AB 375 introduced.
June 28, 2018	<ul style="list-style-type: none">• CCPA is passed and signed into law.
January 1, 2020	<ul style="list-style-type: none">• CCPA goes into effect.
July 1, 2020, or six months after final regulations published, whichever is earlier	<ul style="list-style-type: none">• Enforcement begins. This is not a grace period. The state has the right to bring enforcement actions involving noncompliance starting January 1, 2020.

CCPA California AG's Office Rulemaking Activity

- California AG's Office is hosting public forums to allow interested members of the public to read their comments into the record.
- Website available at: <https://oag.ca.gov/privacy/ccpa>.
- Comments may also be submitted via email or regular mail by March 8, 2019. These comments are subject to the Public Records Act.
- California AG's Office anticipates publishing Notice of Proposed Regulatory Action in the fall of 2019.
- There are specific areas set out by the CCPA for AG Rulemaking:
 - Updating categories of Personal Information
 - Considering any additional exceptions needed to harmonize the CCPA with existing laws
 - Establishing rules and procedures regarding the consumer "opt-out" right
 - Establishing rules for notices to be provided to consumers
 - Establishing rules to enable the Consumer's right to receive certain information

Overview of CCPA



Actions Covered by CCPA

- Provides rights to Consumers regarding their Personal Information as provided by CCPA.
- Understanding how CCPA applies will require understanding the information flow.
- The responsibilities imposed upon an entity, and what that entity will be able to do with personal information will depend on:

Whether the entity has Personal Information (as defined by CCPA).

Who the entity received the Personal Information from.

What rights the upstream provider of Personal Information (consumer or entity) has provided or denied, including through contract or opting out.

Many entities will have multiple data flows, and different corresponding rights and responsibilities as to each data flow.

Actions Covered By The CCPA: Who is a Consumer?

- A “**consumer**” is “a natural person who is a **California resident**, as defined in Section 17014 of Title 18 of the California Code of Regulations . . . , however identified, including by any unique identifier.”
- Per these state regulations, a **California resident** is any individual who is (1) “in the state of California for other than a temporary or transitory purpose,” or (2) “domiciled in the state” of California and “outside of the state for a temporary or transitory purpose.”
- This is a broad definition. Note that a Consumer does not need to be engaging in a commercial activity to be a consumer.
- Personal Information originates from a Consumer. Understanding the data flow will require understanding who the Consumer is.

Overview of CCPA: Definition of Personal Information

- Personal Information is defined as “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.”
- The term "household" is not defined. It could include residences outside of the state of California where a California resident is currently housed, as well as any connected devices within those households that contain Personal Information about California residents.
- CCPA includes examples of Personal Information including: commercial information, including purchase histories, internet and network activity including search history, browsing history, interactions with apps, websites, or advertisements, geolocation data, profiles created from other Personal Information about a consumer.
- On August 31, 2018, via SB-1121, the California State Legislature made certain amendments to the CCPA. One of these was to clarify that these categories would only be Personal Information where they were linked or linkable to a consumer or household.

Overview of CCPA: Personal Information Exclusions

- CCPA excludes certain types of information that would otherwise meet the definition of Personal Information. Such exclusions include information regulated by:
 - HIPAA (Protected Health Information)
 - Information regulated by GLBA
 - Exclusion does not apply to private right of action (SB 1121)
 - Information pursuant to the Driver's Privacy Protection Act of 1994
 - Exclusion does not apply to private right of action (SB 1121)
 - The clinical trials Common Rule
- Further excludes information made “publicly available” that is “lawfully made available from federal, state, or local government records, if any conditions associated with such information.” Information is not “publicly available” if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.

Overview of CCPA: Does Not Apply to Aggregate Consumer Information or Deidentified Data

- If data is “deidentified” such that it cannot be linked to a specific consumer, then it becomes “deidentified data” and CCPA does not apply.
- CCPA requires the use of technical safeguards and business processes to be used to prevent reidentification of this type of data.
- Similarly, CCPA does not apply to “aggregate consumer information” defined as “information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.”
- When designing a business process or data flow, always consider whether deidentified or aggregate data could serve the business purpose.



Overview of CCPA: Collecting and Selling Personal Information

- Does Your Entity Collect Consumer Personal Information?
 - If your entity buys, gathers, rents, obtains, receives, or even accesses Consumer Personal Information, by any means, whether actively or passively, including by observing a Consumer's behavior, then it is collecting Consumer Personal Information.
- Is Your Entity Selling Personal Information?
 - Selling of Consumer Personal Information will occur where your entity is “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]” for “monetary or other valuable consideration.”
 - Note that “Selling” excludes for “use for a business purpose” where used by the business or a service provider for an operational purpose “reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed” or some other compatible operation purpose.
 - Seven specific business purposes are listed within CCPA.

CCPA Obligations by Entity Type



CCPA Entity Types – Understanding the Relationships Between the Three Entity Types

- CCPA imposes burdens on three different types of entities:
 - Businesses
 - Service Providers
 - Third Parties
- Much of the analysis has concerned what Businesses will need to do to comply, however it is important to consider what obligations may be imposed by the other two categories as well.
- A given entity could fall under all three categories, depending on its activities. Many entities will have more than one type of data flow subject to CCPA.
- Most Businesses will take advantage of one or more Service Providers.
- Many Service Providers may also be Businesses under CCPA because of employee information.

CCPA Entity Types: Is Your Entity a “Business” Under the CCPA?

- Are **each** of the following true?
 - Your entity **collects Personal Information from Consumers**, or another entity collects it for you.
 - **You determine**, or do so with others, **the purpose and reason for processing Consumer Personal Information**. Note this is a key distinction between Business and Service Providers. Service providers take their instructions from the Business.
 - **You do business in California**. While not defined by the CCPA, it is reasonable to assume that this would apply to any business who collects Personal Information from a Consumer. Thus, the Business does not need to be geographically located in California.
- Are **one or more** of the following true?
 - You have annual gross revenues in excess of \$25,000,000.
 - You annually buy, share or receive for commercial purposes, or sell, the personal information of more than 50,000 consumers, including households and devices.
 - You receive 50 percent or more of your annual revenue from selling of consumers' personal information.

CCPA Entity Types: Is Your Entity a Service Provider Under the CCPA?

- Most every Business will use one or more Service Providers.
- **Service Providers** are entities that “**processes** information **on behalf of a business** and to which the business **discloses** a consumer’s **personal information** for a business purpose pursuant to a **written contract**.”
- The written contract must prevent the Service Provider from “from retaining, using, or disclosing personal information for any purpose,” other than that of performing the services provided for by the contract.
- Further, Businesses must obligate their Service Providers to “direct any service providers to delete the consumer’s personal information from their records” when a consumer requests that the Business do so.

CCPA Entity Types: Is Your Entity A Third Party Under the CCPA?

- CCPA describes what a “third party” is not.
- A “Third Party” is any entity that is not a CCPA Business, nor a Service Provider, but still receives a Consumer’s Personal Information from the Business.
- Consumers can only opt out of the providing of their Personal Information to Third Parties, not Service Providers.
- Third Parties cannot sell Personal Information about a Consumer sold to it by a Business unless the Consumer has been provided explicit notice regarding the opportunity to opt out of the sale.



CCPA Consumer Rights



CCPA Consumer Rights: Overview

- The CCPA provides dramatic changes to the rights granted to Consumers.
- Businesses need to support the following rights:
 - Disclosure/Privacy Policy Requirements
 - Access/Data Portability
 - Deletion
 - Opt Out Requirements/Non-discrimination
- These rights apply to all Personal Information collected from Consumers by a Business.
- Service Providers will need to be able to support these rights.
- Businesses need to be able to ensure their processes and contracts will enable them to meet these requirements.
- Third Parties will want to protect themselves via contract and due diligence as to any data they receive.

CCPA Consumer Rights: Disclosure/Privacy Policy Requirements

- Before or at the time of collection, a Business must:
 - Inform Consumers of the categories of Personal Information to be collected.
 - Inform Consumers of the purposes for which the categories of Personal Information shall be used.
 - Provide notice of the collection of any additional categories of information or use of collected information for any additional purposes taking place after initial disclosures have been made.
- Privacy Policy Requirements
 - A listing of Consumers' rights under the CCPA, including the consumer right to opt out of the sale of the Consumer's Personal Information and a separate link to the "Do Not Sell My Personal Information" on the Business's website.
 - How Consumers may submit requests to exercise their rights to the Business.
 - A list of the categories of Personal Information that the Business has collected about Consumers, sold about Consumers, and disclosed about Consumers for a business purpose in the preceding 12 months.

CCPA Consumer Rights: Access/Data Portability

- Upon a Verifiable Consumer Request No More Than Twice Per Year
 - Businesses That Collect Personal Information About the Consumer Must Provide:
 - Categories, sources, and business or commercial purpose for collecting of Personal Information the Business has collected about the Consumer
 - Categories of third parties with which the business shares Personal Information
 - Disclose and **provide specific pieces** of Personal Information the Business has collected about the Consumer.
 - Business must provide Personal Information in “readily usable format” that allows porting the data over to another entity “without hindrance.”
 - Businesses are not required to retain information that is obtained in a one-time transaction or to re-identify or link information that is not in identifiable form.
 - Businesses That Sell Personal Information About the Consumer Must Provide:
 - Categories of Personal Information the Business has collected about the Consumer
 - Categories of Personal Information the Business has sold about the Consumer
 - Categories of Third Parties that the Personal Information was sold by category or categories of Personal Information for each third party to which the personal information was sold
 - Categories of personal information the Business has disclosed about the Consumer for a business purpose

CCPA Consumer Rights: Deletion

- Can request deletion of Personal Information (from Business and its Service Providers)
- The CCPA provides that Consumers can request that a Business delete **any** Personal Information about the Consumer, so it may be that Consumers can request partial deletions.
- Many exceptions are present.
 - Necessary to provide a good or service requested by the Consumer or reasonably anticipated due to relationship with the Consumer.
 - Detecting security incidents or fraud, as well as debugging existing intended systems.
 - Enabling internal uses that are aligned with Consumer expectations based on the relationship.
 - Complying with legal obligations.
 - These exceptions could be construed to be fairly broad in nature, particularly as they relate to detecting fraud, and debugging systems.

CCPA Consumer Rights: Opt Out Requirements/Non-Discrimination

Opt Out

The CCPA authorizes a Consumer to opt out of the sale of Personal Information by a Business. Businesses must make available, in a form reasonably accessible to Consumers, a “clear and conspicuous link to the homepage”, titled “Do Not Sell My Personal Information.” That link must go to a webpage that enables the Consumer to opt out. The Business must wait a minimum of 12 months before requesting to sell the Personal Information of a Consumer who has opted out.

Non-Discrimination

Businesses are prohibited from discriminating against the Consumer for exercising this right, including by charging the Consumer who opts out a different price or providing the Consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the Consumer’s data. Financial incentives offered to the Consumer for the collection, sale, or deletion of Personal Information are permitted only with the prior opt in by the Consumer.

Enforcement of CCPA



Enforcement of the CCPA: CA Attorney General

- **CA Attorney General**

- **Violations Generally:** Authority to bring action for up to \$2,500 for any violation of CCPA.
- **Damages:** Calculated on a per-capita basis. For example, if a violation affects 1,000 users, damages could rise to \$2,500,000.
- **Intentional Violations:** For violations viewed as intentional, the Attorney General's office may bring an action for up to \$7,500 for any violation of the CCPA. The same 1,000 users could be awarded damages of \$7,500,000.
- **Notice and Cure Period**
 - Entity has 30 days after receiving notice of noncompliance from the California Attorney General's office to cure it, and only thereafter are they subject to an enforcement action for violating CCPA.

Enforcement of the CCPA: Private Right of Action

- **Private Right of Action**

- **Consumer:** May bring civil action for alleged failure to “implement and maintain reasonable security procedures and practices” by Business that results in a data breach of non-encrypted or non-redacted Personal Information.
- **Individual or Class Action:** Action may be brought as class action or on an individual basis.
- **Damages:** CCPA provides for statutory damages between \$100 and \$750 or actual damages.
- **Notice and Cure Period:**
 - Consumer must provide Business 30 days to cure the alleged violation.
 - If the Business actually cures the violation within 30 days, no action may be initiated.
 - No notice shall be required prior to an individual Consumer initiating an action solely for actual damages suffered.

CCPA Compliance Strategies



CCPA Compliance Strategies

- Understand how Personal Information flows through your organization.
- **Points of Collection:** Have privacy policies or other mechanisms been updated to disclose what information is being collected, disclosed, and sold? Does the privacy policy provide a disclosure of the right to opt-out of any such selling? Does it explain the new Consumer rights provided by the CCPA?
- **Data Management:** Complying with the CCPA will require understanding where Personal Information is at any given time. Companies will need mechanisms to track business processes, products, devices, applications and third parties that access the Personal Information of Consumers.
- **Support for Consumer CCPA Rights:** The rights of Access/Data Portability, Deletion, Opt Out Requirements/Non-discrimination will require support throughout the organization, and at the information technology infrastructure level.
 - **Consumer Requests:** Verify, document and support requests.
 - **Create Systems of Record:** This will serve as a record of the execution of Consumer requests.
 - **Provide Training:** Stakeholders must be informed and empowered to act.
 - **Testing:** Test processes and controls before January, 2020.

CCPA Compliance Strategies

- **Information Security:** Identify and close any security gaps.
 - The CCPA will greatly increase the cost of non-remediated gaps through its statutory damages provision within the private right of action.
 - Being able to track where data was, and attest that it was not breached will be important for limiting exposure.
- **Service Provider Agreements:** Create a process for reviewing current and future contracts and negotiating necessary CCPA amendments. Remember that if appropriate provisions are not in place, there is the possibility that the vendor may not be considered a Service Provider under the CCPA.
 - Service Provider must refrain “from retaining, using, or disclosing personal information for any purpose,” other than that of performing the services provided for by the contract.
 - Service Provider must agree to support Consumer CCPA rights, including Access/Portability, Deletion, and Opt-outs.

CCPA Compliance Strategies

- **Business Model Analysis:** Consider whether any portion of the CCPA would motivate the redesign of a business process or external offering.
 - How will the antidiscrimination provisions be dealt with?
 - How will the Business calculate the value provided by the Consumer's data?
 - How would the offering of financial incentives to the Consumer for the collection or sale of Personal Information impact the viability of the Business?
- **Achieve Corporate Buy-In**
 - Culturally, how does the Business plan to make CCPA compliance a priority while demonstrating its value to stakeholders?
 - Can the Business use its newly created CCPA processes as a competitive advantage?



MINTZ

THANK YOU

[Click here to subscribe to our blog](#) for updates and more information.

Join us on March 27th for our next webinar:
Is the CCPA really “GDPR-Lite”?