



PROGRAM MATERIALS
Program #29165
October 21, 2019

CCPA: The More Things Change, The More Things Stay the Same

**Copyright ©2019 by Sadia Mirza, Esq. - Troutman
Sanders. All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969



California Consumer Privacy Act

The More Things Change, the More
Things Stay the Same

Sadia Mirza, CIPP/US
October 21, 2019

Opening Credits



Sadia Mirza, CIPP/US

Attorney, Troutman Sanders LLP

Sadia Mirza is part of the Cybersecurity, Information Governance and Privacy practice group at Troutman Sanders, and is also part of the Financial Services Litigation practice group. She provides strategic privacy compliance counseling, and defends, counsels and represents companies on matters relating to data privacy, data use, and incident response and investigation, with an eye towards helping clients avoid litigation. Additionally, she has experience with the California Consumer Privacy Act of 2018 (CCPA), the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), as well as various other laws concerning privacy and cybersecurity. Sadia's in-house background allows her to understand the issues and concerns clients have and guide them toward resolution in a clear and efficient way. She has worked with clients from a variety of industries, including financial institutions, consumer reporting agencies, insurance companies, healthcare providers, and data and analytics providers. Prior to becoming an attorney, Sadia worked for JPMorgan Chase and Washington Mutual Bank.

Roadmap



Big Picture



Important Dates



CCPA In-Detail



Amendments



Further Legislation



Key Takeaways



Big Picture

- ▶ Global shift towards more comprehensive legislation on data privacy.
- ▶ The European Union's General Data Protection Regulation ("GDPR") became effective May 25, 2018.
- ▶ **However, despite the rumors, the CCPA is not Europe's fault.**
- ▶ CCPA is based on Fair Information Practice Principles (FIPS), which is the foundation for most privacy laws in the US and internationally.

California Consumer Privacy Act of 2018 (CCPA)

- ▶ Effective January 1, 2020
- ▶ Applies to companies collecting personal information on California consumers
- ▶ Increased transparency
- ▶ Gives California consumers greater control over Personal Information
- ▶ Penalties and enforcement actions for CCPA violations
- ▶ New statutory damages for data breaches



Important Dates

Signed: June 29, 2018

Initially Amended: September 23, 2018

Effective Date: January 1, 2020

“Lookback” Date: January 1, 2019

AG Enforcement Date: As late as July 1, 2020

- Private right of action for data breaches still effective as of January 1, 2020.

More Amendments: Signed Into Law by Oct. 13 2019

Who Must Comply?

“Business”

- ▶ Directly or on behalf of other entity collects and determines purposes and means of processing and does business in CA and meets at least one of the below:
 - ▶ Annual gross revenues > \$25 MM; or
 - ▶ Buys, receives or shares for commercial purposes, or sells personal information of 50,000 or more consumers, households, or devices; or
 - ▶ Derives 50% or more of annual revenues from selling consumers' personal information.
- ▶ Includes entities controlled by a business and that shares common branding with the business, even if not otherwise covered.
- ▶ Definition has a wide reach - not only limited to businesses incorporated in California.

Who Must Comply?

- “Service Provider”

- ▶ Means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, 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, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

- “Third Party”

- ▶ Not the business that collects personal information from consumer.
- ▶ Not the person to whom business discloses a consumer’s personal information for a business purpose pursuant to written contract.
- ▶ Cannot resell personal information, unless consumers have received notice and opportunity to opt out.

What Does it Cover?



What Does it Cover?



- Covers California “Consumers”
 - ▶ Definition: means natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.
 - ▶ Implications:
 - ▶ Any resident according to the California tax code.
 - ▶ Empl
 - ▶ Businesses should think about how they will identify their California consumers while crafting CCPA compliance programs.

What Does it Cover?

“Personal Information”

- ▶ Definition: means 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. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:
 - ▶ 11 categories provided of examples of personal information provided - not an exhaustive list.
 - ▶ “Household” is not defined.
- ▶ Exemptions:
 - ▶ **Publicly Available Information** - records made available from federal, state, or local government records.
 - ▶ Personal Information likely does not include consumer information that is **deidentified** or **aggregate consumer information**.
 - Both terms are defined under the CCPA.

What Does it Cover?

- **“Collecting”**
 - ▶ Includes: buying, renting, gathering, obtaining, receiving, or accessing any personal information
 - ▶ Includes actively or passively receiving information
- **“Selling”**
 - ▶ Includes: selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating
 - ▶ Provided to third party for “monetary or other valuable consideration”
 - ▶ Exceptions
- No data minimization requirement like the GDPR



Obligations

▶ Access

- ▶ Section 1798.100(a)
- ▶ Section 1798.110(b)
- ▶ Section 1798.115(a)

▶ Portability

- ▶ Section 1798.100(d)

▶ Deletion

- ▶ Section 1798.105

▶ Opt Out and Opt In for Sale of Personal Information

- ▶ Section 1798.120

▶ No Discrimination

- ▶ Section 1798.125

Access

Section 1798.100(a)

- Categories of personal information collected.
- Specific pieces of personal information collected.

Section 1798.110(b)

- Categories of personal information collected about consumers.
- Categories of sources from which the personal information is collected.
- Business and commercial purposes for collecting or selling personal information.
- Categories of third parties with whom the business shares personal information.
- That a consumer has the right to request the specific pieces of personal information a business has collected about that consumer.



Portability

- Section 1798.100(d)
 - “A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, *the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance.*”

Deletion



- **Section 1798.105(a)**
 - ▶ “A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”
- **Certain exemptions apply**
 - ▶ Exercise free speech
 - ▶ Detect security incidents
 - ▶ Complete the transaction for which the personal information was collected
 - ▶ Comply with a legal obligation
 - ▶ See 1798.105(d) for other exemptions



Opt Out and Opt In of Sale of PI

- Section 1798.120
- Authorizes consumers to opt out of the sale of their personal information.
- For children “less than 16 years of age,” businesses must obtain “affirmative authorization” before selling their personal information.
 - ▶ Expands on the protections provided to minors under the Children’s Online Privacy Protection Act (COPPA).

Provide a clear and conspicuous link on homepage and in privacy policy: “Do Not Sell My Personal Information.”

- ▶ Pay attention to how “homepage” is defined

Notice Requirements

Just-in-Time Notice

- Section 1798.100(b)
- “At or before the point of collection”
- Notice required even in brick-and-mortar stores

Privacy Policy

- Sections 1798.110(c) and 1798.130(a)(5)
- Update every 12 months
- Include a description of rights pursuant to Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 and one more more designated methods for submitting requests

Verifiable Consumer Request

- Most obligations triggered upon a “Verifiable Consumer Request”
 - ▶ Section 1798.100(c) - Limited Access
 - ▶ Section 1798.105 - Delete
 - ▶ Section 1798.110(b) - Full Access
 - ▶ Section 1798.115(b) - Onward Disclosures
- Time to Comply
 - ▶ Generally, 45 days of receiving a verifiable consumer request from the consumer.
- Further Guidance
 - ▶ AG to adopt regulations pursuant to 1798.185(a)(7) to establish rules and procedures governing what constitutes a “verifiable consumer request.”

Exemptions

- ▶ CCPA does not apply to:
 - ▶ Certain medical information.
 - ▶ Sale of personal information to or from a consumer reporting agency and use is limited by FCRA.
 - ▶ Personal information collected, processed, sold, or disclosed pursuant to GLBA or the California Financial Information Privacy Act (except for data breach private right of action).
 - ▶ Personal information collected, processed, sold, or disclosed pursuant to DPPA (except for data breach private right of action).

Exemptions

- ▶ Shall not restrict ability to:
 - ▶ Use deidentified or aggregated consumer information
 - ▶ Compliance with federal, state or local laws
 - ▶ Compliance with investigation, subpoena, summons by regulators or state or local authorities
 - ▶ Exercise or defend legal claims
 - ▶ Cooperate with law enforcement
 - ▶ Abide by evidentiary privilege



Enforcement

▶ Data Breaches - Private Right of Action

- ▶ Enforcement for Section 1798.81.5 - California's Data Breach statute
- ▶ Damages in amount not less than \$100 and not greater than \$750 per consumer per incident or actual damages, whichever is greater
- ▶ Information collected pursuant to FCRA, GLBA and DPPA not exempt from this section

▶ CCPA Violations - AG Enforcement

- ▶ Civil penalty of not more than \$2,500 for each violation or \$7,500 for each intentional violation
- ▶ Hotly debated issue

AG Regulations

▶ **AG required to promulgate further regulations by July 1, 2020 on the following issues:**

- Authorizing another person to opt-out of sale of consumer's personal information on consumer's behalf.
- Providing additional "designated methods for submitting requests."
- Methods for verifying a consumer request.
- Any additional regulations "as necessary."



Amendments
that Made it
to the Finish
Line (Almost)

AB 25 - Personal Information in Employment Context

- ▶ Temporarily excludes, until January 1, 2021, personal information collected in the **employment context** from the scope of the CCPA, except with respect to the CCPA's private right of action relating to data breaches and notice obligations pursuant to Section 1798.100.
- ▶ The private right of action (breach) and notice obligations under Section 1798.100 will continue to take effect on January 1, 2020 with respect to personal information collected in the employment context (and personal information collected otherwise).
- ▶ Expressly specifies an exemption for PI collected and used solely for emergency contact purposes and where the PI is necessary to be retained for the administration of benefits.
- ▶ Clarifies the authority that a business has to require reasonable authentication of a consumer and to use existing account of consumers to convey CCPA requests.

AB 874 - Redefining PI and “Publicly Available”

- ▶ Expands the scope of “publicly available” information that is exempted from the PI definition to ensure that “publicly available” includes any information that is lawfully made available from government records. In other words, it removes the conditions previously associated with “publicly available” information.
- ▶ Amends the PI definition to: (1) correct a drafting error in order to clarify that PI (as opposed to “publicly available” information) does not include deidentified or aggregate consumer information; and (2) specifies, in relevant part, that PI includes information that is “*reasonably* capable” of being associated with a particular consumer or household, as opposed to “capable” of being associated.

AB 1146 - Vehicle Warranties, Repairs, and Recalls



- ▶ Creates an exception to the right to opt out for vehicle information or ownership information retained or shared between a new motor vehicle dealer and the vehicle's manufacturer, if the information is shared for the purpose of a vehicle repair covered by warranty or a recall.
- ▶ Creates an exception to the right to deletion for personal information that is necessary to maintain in order to fulfill the terms of a written warranty or a product recall in accordance with federal law.

AB 1202 - Data Broker Registry

- ▶ Requires data brokers to register with and provide certain information to the California Attorney General and requires the AG to create a publicly available registry of data brokers on its website.
- ▶ Makes data brokers that fail to register subject to injunction and liability for civil penalties, fees, and costs in an action brought by the AG.
- ▶ Defines a “data broker” as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. “Data brokers” does not include any of the following:
 - ▶ (1) a consumer reporting agency covered by the Fair Credit Reporting Act (“FCRA”);
 - ▶ (2) a financial institution covered by the Gramm-Leach-Bliley Act (“GLBA”); and
 - ▶ (3) an entity governed by the Insurance Information and Privacy Protection Act.
- ▶ Provides that the bill shall not be construed to supersede or interfere with the CCPA.

AB 1355 - The Clarification Amendment

- ▶ Refines the existing FCRA exemption so that it applies to any activity involving collection, maintenance, disclosure, sale, communication, or use of any PI bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, only to the extent such activity is subject to the FCRA, but prevents application of this exception to the CCPA's private right of action.
- ▶ Specifies that, until January 1, 2021, certain CCPA obligations do not apply to PI reflecting a communication or transaction between the business and the consumer, where the consumer is a natural person: (1) who is an employee, owner, director, officer, or contractor of a government agency or a business; and (2) whose communications or transactions with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from that business or government agency (*i.e.*, "business-to-business" communications or transactions).
- ▶ Addresses various other non-substantive drafting errors.

AB 1564 - Designated Methods to Submit Certain Information Requests



- ▶ Updates the designated methods to submit consumer requests to no longer require a telephone number in all instances. Specifically, if a business operates exclusively online and has a direct relationship with consumers, it is only required to provide an email address for submitting certain requests.
- ▶ Requires businesses that maintain an internet website to make the website available to consumers to submit certain requests.

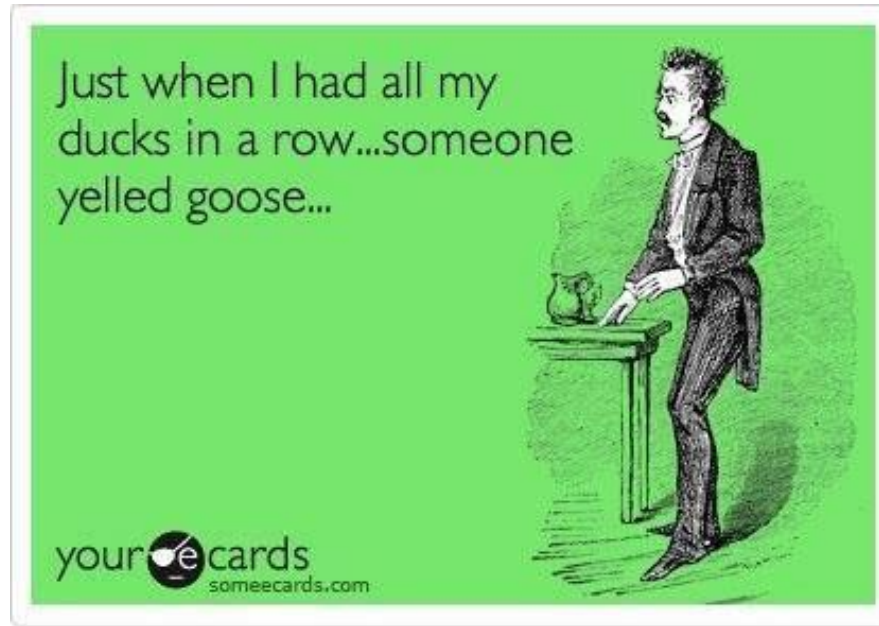
Other Legislative Efforts Following CCPA

Examples

- Hawaii S.B. 418
- New York S.B. 224
- Nevada S.B. 220 (Effective October 1, 2019)
- Massachusetts S.B. 120
- Maryland S.B. 613
- Illinois S.B. 2149

Key Takeaways

- While the privacy landscape is uncertain at the moment, the focus is clearly on greater access to information and transparency.
- Identifying what personal information a business has, where it came from, where such information flows, and for what purposes are the key steps to compliance with the CCPA and CCPA-like laws.
- Be considerate of other privacy legislation (both enacted and proposed) when crafting CCPA-compliance programs. Businesses should consider:
 - ▶ The advantages and disadvantages of establishing a universal privacy management framework.
 - ▶ How differences in the proposed CCPA-like laws may further complicate prospective compliance efforts (e.g., variances in how exceptions are applied).



Questions?



Sadia Mirza, CIPP/US

Troutman Sanders LLP

sadia.mirza@troutman.com

949.622.2786