

**SUMMARY OF CALIFORNIA CONSUMER
PRIVACY ACT OF 2018**

Civil Code Sections 1798.100 et seq.

NOSSAMAN LLP

THOMAS DOVER

STEPHEN P. WIMAN

March 2019

CONTENTS

	Page
INTRODUCTION.....	3
EXECUTIVE SUMMARY	4
DETAILED SUMMARY OF THE CCPA.....	8
TO WHOM DOES THE CCPA APPLY?.....	9
Consumers	9
Businesses	9
INFORMATION SUBJECT TO THE CCPA.....	11
RIGHTS AND OBLIGATIONS UNDER THE CCPA	13
Rights Of Consumers	13
Obligations Of Businesses.....	14
NON-DISCRIMINATION AND FINANCIAL INCENTIVE	18
WHAT IS THE LIABILITY EXPOSURE FOR A VIOLATION OF THE CCPA?.....	19
California Attorney General Enforcement	19
Private Consumer Enforcement.....	19
EXCLUSIONS FROM THE CCPA	23
DOES SALE INCLUDE MERGER, ACQUISITION, OR BANKRUPTCY?.....	24

INTRODUCTION

In 2018, the California Legislature enacted the California Consumer Privacy Act of 2018, Civil Code, § 1798.10 et seq., effective January 1, 2020. The statute is the byzantine manifestation of an effort to thwart a much more severe ballot initiative that was withdrawn because of the enactment of the statute.

The statute seeks to protect the dissemination by sale and disclosure of information related to California residents (defined as “consumers” in the statute) and provides certain rights to consumers to control the use, sale and disclosure of that information. At the same time, the statute imposes obligations upon “businesses” to disclose to consumers on request information regarding collection, use and sale of personal information.

Overall, the California Attorney General is responsible for enforcing the statute. Complementing this public enforcement, the statute creates a private right of action in consumers authorizing them to sue businesses who have experienced a data breach by reason of a failure to implement and maintain reasonable security procedures and practices.

The statute is not well drafted; it is verbose and ambiguous. On or before January 1, 2020, the Attorney General is required to adopt regulations to further the purposes of the statute.

Pending amendments to the statute appear intended to make the statute even more draconian than it currently is.

Certain terms used in this summary have been italicized to reflect that the terms have a formal definition in the statute itself. The definitions are extensive and contained in section 1798.140 of the Civil Code. When reading the actual language of the statute, one should have a copy of that section at hand.

What follows is an Executive Summary taken from the Legislative Counsel’s Digest of the CCPA. Behind the Executive Summary is a more detailed summary.

EXECUTIVE SUMMARY OF THE CCPA

The Legislative Counsel's Digest provides:

The California Constitution grants a right of privacy. Existing law provides for the confidentiality of personal information in various contexts and requires a business or person that suffers a breach of security of computerized data that includes personal information, as defined, to disclose that breach, as specified.

This bill would enact the California Consumer Privacy Act of 2018. Beginning January 1, 2020, the bill would grant a consumer a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared.

The bill would require a business to make disclosures about the information and the purposes for which it is used.

The bill would grant a consumer the right to request deletion of personal information and would require the business to delete upon receipt of a verified request, as specified.

The bill would grant a consumer a right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose the categories of information that it collects and categories of information and the identity of 3rd parties to which the information was sold or disclosed.

The bill would require a business to provide this information in response to a verifiable consumer request.

The bill would authorize a consumer to opt out of the sale of personal information by a business and would prohibit the business 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.

The bill would authorize businesses to offer financial incentives for collection of personal information.

The bill would prohibit a business from selling the personal information of a consumer under 16 years of age, unless affirmatively authorized, as specified, to be referred to as the right to opt in. The bill would prescribe requirements for receiving, processing, and satisfying these requests from consumers.

The bill would prescribe various definitions for its purposes and would define "personal information" with reference to a broad list of characteristics and behaviors, personal and commercial, as well as inferences drawn from this information.

The bill would prohibit the provisions described above from restricting the ability of the business to comply with federal, state, or local laws, among other things.

The bill would provide for its enforcement by the Attorney General, as specified, and would provide a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information, as defined.

The bill would prescribe a method for distribution of proceeds of Attorney General actions.

The bill would create the Consumer Privacy Fund in the General Fund with the moneys in the fund, upon appropriation by the Legislature, to be applied to support the purposes of the bill and its enforcement.

The bill would provide for the deposit of penalty money into the fund.

The bill would require the Attorney General to solicit public participation for the purpose of adopting regulations, as specified.

The bill would authorize a business, service provider, or 3rd party to seek the Attorney General's opinion on how to comply with its provisions.

The bill would void a waiver of a consumer's rights under its provisions.

DETAILED SUMMARY OF THE CCPA

TO WHOM DOES THE CCPA APPLY?

Consumers

The CCPA protects “*consumers*” which the statute defines in relevant part as “a natural person who is a California resident” In short, the CCPA applies to individuals who reside in California. There is no other limiting factor contained in the statute. (Civ. Code, § 1798.140(g).)

Questions/Comments:

Given the broad definition of *consumer* and the definition of *personal information* as including “employment related information,” there is a question as to whether the statute applies to information that businesses maintain on their California employees.

Businesses

The CCPA applies to a “*business*” that

- * is organized or operated “for the profit or financial benefit of its shareholders or other owners;”
- * *collects consumers’ personal information* “or on behalf of which such information is collected;”
- * does business in the State of California; and
- * satisfies one or more of the following thresholds:

Has annual gross revenues in excess of \$25,000,000; **or**

“Alone or in combination, annually buys, receives for the *business’* [sic] *commercial purposes*, *sells*, or shares for *commercial purposes*, alone or in combination, the *personal information* of 50,000 or more *consumers*, households, or *devices*”; **or**

“Derives 50 percent or more of its annual revenues from *selling consumers’ personal information.*”

Business includes certain related entities of the business. Thus, the statute applies to any entity that is controlled (as defined in the statute) by a “business” as defined and that shares common branding with the business. “Common branding means a shared name, servicemark, or trademark.” (Civ. Code, § 1798.140(c).)

Questions/Comments:

1. How is the threshold of \$25,000,000 calculated? Is it revenue generated within California or anywhere? Does it include revenue of a subsidiary that shares a common branding with the parent?

2, “Household” is not defined. What is included in a “household” and how does a business determine it is dealing with a household?

INFORMATION SUBJECT TO THE CCPA

The CCPA is not limited to sensitive person data. The statute applies to all “personal information” (collected by whatever means – Internet or otherwise) that can be reasonably linked to a California resident or California household. (Civ. Code, § 1798.140(o)(1) and § 1798.175.)

Information subject to the statute includes, among other things,

- * identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number;

- * 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 an Internet Web site, application or advertisement;

- * geolocation data;

- professional or employment-related information;

- * education information

- * inferences drawn from the foregoing information to create a profile about a *consumer* reflecting the *consumer’s* preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

The CCPA does not apply to information that has been made publicly available through government records. (Civ. Code, § 1798.140(o)(2).)

Questions/Comments:

Given the broad definition of *consumer* and the definition of *personal information* as including “employment related information,” there is a question as to whether the statute applies to information that businesses maintain on their California employees, Whether regulations address this remains to be seen.

RIGHTS AND OBLIGATIONS UNDER THE CCPA

Rights Of Consumers

* Notice of the *personal information collected* and the purpose for *collecting* such category of information, at or prior to the collection of the information. (Civ. Code, § 1798.100(b).)

* Request that a *business* that *collects personal information* disclose the categories of such information collected, the categories of sources from which the information is collected, the business or commercial purpose for *collecting* or *selling* information, the categories of *third parties* with whom the *business* shares information, the specific pieces of information collected about the particular *consumer* and provide copies of such information. (Civ. Code, § 1798.100(a) and § 1798.110(a).)¹

* Request that a *business* that *sells* or discloses *personal information* disclose the categories of *personal information* sold or disclosed, the categories of *third parties* to whom the *personal information* was sold. (Civ. Code, § 1798.115(a).)

* Request that a *business* that *collects personal information* delete, subject to certain exceptions, any *personal information* about the *consumer* that the *business* has *collected*, (Civ. Code, §1798.105)(a).)

* Notice from a *business* that *sells personal information* that the *business* may *sell* the information and that the *consumer* has the right to opt out of such sales. (Civ. Code, § 1798.120(b).)

* Direct that a *business* that *sells personal information* to *third parties* not *sell* the *consumer's* information (opt out right); the *business* must follow the direction. (Civ. Code, §1798.120(a) and (c).) A *business* shall refrain from *selling personal information* of a *consumer* who opts out. (Civ. Code, § 1798.135(a)(4).) Following an opt out, a *business* shall wait

¹ The CCPA defines “third party” in a bizarre manner. It states what a third party is not, namely, a third party is not a *business* or a *service provider* as defined in the statute. (Civ. Code, § 1798.140(w).)

one year before requesting that the *consumer* authorize the *sale* of *personal information*. (Civ. Code, § 1798.135(a)(5).)

* Notice of from a *third party* that *sells personal information* that the *third party* may *sell* the information and that the *consumer* has the right to opt out of such sales. (Civ. Code, § 1798.115(d).)

Obligations Of Businesses

The obligations of *businesses* subject to the CCPA mirror the rights of *consumers*.

* A *business* that *collects personal information* from *consumers* must notify *consumers*, at or before the time of *collection*, what categories of *personal information* will be *collected* and the purposes for which each category of *personal information* will be used. (Civ. Code, § 1798.100(b).)

* Upon receipt of a *verifiable consumer request*, a *business* must disclose the categories of such information collected, the categories of sources from which the information is collected, the business or commercial purpose for *collecting* or *selling* information, the categories of *third parties* with whom the *business* shares information, the specific pieces of information collected about the particular *consumer* and provide copies of such information. (Civ. Code, § 1798,110(b) and (c); see also Civ. Code, § 1798.130(a)(3).) A *business* has a similar obligation with respect to such information that it discloses or sells for a *business purpose*. (Civ. Code, § 1798.115(b) and (c); see also § 1798.130(a)(4).)

* Upon receipt of a *verifiable consumer request*, a *business* must respond, disclose and deliver the required information within 45 days subject to an additional 45 days extension or 90 days “where necessary, taking into account the complexity and number of the requests.” The *business* must notify the *consumer* of the extension and the reason for it. “The disclosure shall cover the 12 –month period preceding the business’s receipt of the request and shall be made in writing and delivered through the consumer’s account or by mail or electronically. . . .” (Civ. Code, §

1798.130(a)(2).) A *business* is not required to respond to a request more than twice in a 12 month period. (Civ. Code, §1798.100(d); § 1798.130(b).)

* A *business* is authorized to provide *consumer* requested disclosures only upon receipt of a *verifiable consumer request*. (Civ. Code, § 1798.100(c) and (d).) The *business* is not required to provide disclosures if it is not able to verify that a *consumer* making the request is the *consumer* about whom the *business* has *collected* information or someone authorized by the *consumer* to make the request.

* Subject to a number of exceptions, upon receipt of a *verifiable consumer request* to delete *personal information*, a *business* shall delete that information and direct any *service provider* to delete such information. (Civ. Code, §1798.105(c) and (d).)²

* Information must be delivered to a *consumer* free of charge unless the requests are “manifestly unfounded or excessive . . . because of their repetitive character.” In such an event, the *business* may charge a reasonable fee. (Civ. Code, §1798.100(d).)

* A *business* that *sells personal information to third parties* must notify the *consumer* that the *business* may sell the information and that the *consumer* has the right to opt out of such sales. (Civ. Code, § 1798.120(b).)

² A “service provider” is a business entity operated for profit or financial benefit “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” that limits the *service provider’s* disclosure or use of the information for a purpose other than that set forth in the contract. (Civ. Code, § 1798.140(v); see also Civ. Code, § 1798.140(d) which extensively defines *business purpose* and includes maintaining and servicing accounts, customer service, fulfilling orders.) In discussing the definition of “third party,” Civil Code section 1798.140(w) also sets forth requirements for a *service provider* that appear to prevent such a provider from *selling personal information*; the section also limits a *business’s* exposure to liability if a service provider violates the statute

* A *business* must notify a *consumer* of the *consumer's* right to request the deletion of *personal information*. (Civ. Code, § 1798.105(b).)

* A *business* that has actual knowledge a *consumer* is less than 16 years of age may not *sell* the minor's information unless the *business* obtains particular consents. (Civ. Code, § 1798.120(d).)

* A *business* must provide to *consumers* "two or more designated methods for submitting" disclosure requests which must include "at a minimum, a toll-free telephone number, and if the *business* maintains an Internet Web site, a Web site address." (Civ. Code, § 1798.130(a)(1).)

* A *business* must provide a "clear and conspicuous link on its Internet homepage, titled 'Do Not Sell My Personal Information,'" to an Internet Web page that enables a *consumer*, or a person authorized by the *consumer*, to opt out of the sale of *personal information*; the *business* is also obligated to include a description of a *consumer's* opt out rights. (Civ. Code, § 1798.135(a).)

* A *business* must also ensure that persons "responsible for handling *consumer* inquiries about the business's privacy practices" or compliance with CCPA are informed (a) of the *business's* obligations and the *consumer's* rights under the CCPA and (b) how to direct *consumers* to exercise their rights under the CCPA. (Civ. Code, § 1798.130(a)(6).)

* A *third party* shall not sell *personal information* that has been sold to the *third party* by a *business* unless the *consumer* has received explicit notice and is provided an opportunity to exercise the right to opt out, namely prevent the sale of the information. (Civ. Code, § 1798.115(d).)

* If a *business* has an online privacy policy or, if no such policy, on the *business's* web site, the *business* must include in the policy or website,

a description of *consumer* rights under the CCPA and one or more designated methods for submitting requests;

a list of categories of *personal information* it has collected about *consumers* in the preceding 12 months;

a list of categories of *personal information* it has sold about *consumers* in the preceding 12 months; and

a list of categories of *personal information* it has disclosed about *consumers* for a *business purpose* in the preceding 12 months.

(Civ. Code, § 1798.130((a)(5).)

NON-DISCRIMINATION AND FINANCIAL INCENTIVE

A *business* shall not discriminate against a *consumer* because the *consumer* exercised any of the *consumer's* rights under the statute. (Civ. Code, § 1798.125(a).)

A *business* may offer financial incentives, including payments to *consumers* as compensation, for the collection of *personal information*, the sale of *personal information*, or the deletion of *personal information*. A *business* may also offer different prices, rate level, quality of goods or *services* to a *consumer* that are related to the value provided by the *consumer's* data. (Civ. Code, § 1798.125(b).)

WHAT IS THE LIABILITY EXPOSURE FOR A VIOLATION OF THE CCPA?

California Attorney General Enforcement

The CCPA authorizes, the California Attorney General to sue to enforce violations of the statute following the Attorney General providing the *business* with a 30 day notice of violation that goes uncured. The Attorney General may obtain injunctive relief and a civil penalty of not more than \$2,500 for each violation and \$7,500 for each **intentional** violation. (Civ. Code, § 1798.155(a) and (b).)

It is currently unclear how the Attorney General or the courts will construe a violation, namely whether it is a single act or omission or a series of related acts or omissions that constitute a single violation.

Recovered civil penalties are to be deposited into a Consumer Privacy Fund, to be used exclusively to offset costs incurred by the courts and the Attorney General related to the CCPA. (Civ. Code, 1798.155(c) and (d) and § 1798.160.)

Private Consumer Enforcement

Any *consumer* whose nonencrypted or nonredacted *personal information* is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the *business's* violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the *personal information* may institute a civil action for any of the following:

- * recovery of damages in an amount of not less than \$100 and not greater than \$750 (statutory damages) per *consumer* per incident or actual damages, whichever is greater;
- * injunctive or declaratory relief; and
- * any other relief the court deems proper.

(Civ. Code, § 1798.150(a).)

The definition of “*personal information*” for purposes of a private right of action is narrower than the definition for the other portions of the act. Rather than using the definition of “personal information” in the statute, the act refers to another more narrow section of the Civil Code (section 1798.81.5) outside of the statute. (Civ. Code, §1798.150(a)(1).) The CCPA broadly defines “personal information” to mean any type of nonpublicly available information that can be linked to a *consumer* or household. In contrast, section 1798.81.5 restricts its definition of “*personal information*” to certain specific categories of information.

In assessing the amount of statutory damages per incident of \$100 to \$750, the court is to consider a number of things, “including, but not limited to, the nature and seriousness of the misconduct, the number of violations, **and the defendant’s assets, liabilities, and net worth.**” (Emphasis added.) (Civ. Code, § 1798.150(a)(2).)

Prior to initiating any action for **statutory** damages (as opposed to actual damages), a *consumer* must provide the potential *business* defendant with a 30 day notice identifying the specific violations. (Civ. Code, § 1798.150(b)(1).) “In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the *consumer* an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.” Should the *business* breach the express written statement, the *consumer* can then sue the *business* for statutory damages for each violation of the written statement. (*Ibid.*)

Within 30 days of filing an action against a *business*, the *consumer* must notify the California Attorney General who has the discretion to take over and prosecute the litigation. (Civ. Code, § 1798.150(b)(2) and (3).)

Under the current language of the statute, *businesses* may seek the opinion of the Attorney General for guidance on compliance with the CCPA. (Civ. Code, § 1798.155.)

Questions/Comments:

1. Under the current language of the statute, the private right of action exists only for a *business* breach arising from a failure to maintain reasonable security measures, and not any other failures to comply with the CCPA. There is pending an amendment to the statute in the California Legislature that would allow a private right of action for any violation of the CCPA.

2. Given the reference to “nonencrypted” *personal information*, a *business* subject to the CCPA should consider whether to encrypt the *personal information*.

3. Note that a breach involving 1,000,000 California residents could result in exposure to a potential statutory damage award of between \$100,000,000 to \$750,000,000.

4. The CCPA does not define what constitutes “reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.”

5. The CCPA does not define exfiltration or distinguish it from theft or a violation of the duty to implement and maintain reasonable security procedures and practices.

6. Note that “the defendant’s assets, liabilities, and net worth” may be considered in determining the amount of statutory damages. Exposure to an inquiry into this information, provides substantial leverage to a *consumer* plaintiff in forcing a *business* defendant to settle. There also may be due process controls on application of this standard to the amount of statutory damages similar to what the Supreme Court has imposed on the award of punitive damages, namely, the amount award must bear some reasonable relationship to the actual resulting harm. (*BMW of North America v. Gore* (1995) 517 U.S. 559, 580-581.)

7. As to the referenced notice and a cure, it is unclear what a *business* may do to “cure” a violation if the *personal information* is in the possession of a cyber thief.

8. There is a pending amendment to the CCPA to delete the provision for seeking an opinion from the Attorney General as to compliance.

EXCLUSIONS FROM THE CCPA

The CCPA contains a number of exclusions. (Civ. Code, § 1798.145.) Some of the more significant ones are:

- * Medical and health information which federal law regulates (HIPAA);
- * Information collected as part of a clinical trial subject to federal law;
- * Sale of *personal information* “to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report” subject to the Fair Credit reporting Act;
- * *Collection, use, retention, sale or disclosure of consumer information* that is “*deidentified*” (“information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked . . . to a particular consumer, subject to certain procedural protections) or in the aggregate consumer information” (“information that relates to a group or category of consumers, from which individual consumer identities have been removed”)³

³ See Civil Code section 1798.140(a) and (h) for definitions of *aggregate consumer information* and *deidentified*, respectively.

DOES SALE INCLUDE MERGER, ACQUISITION, OR BANKRUPTCY?

What happens if there is a transfer of *personal information* as part of a merger, acquisition, bankruptcy or other transaction where a *third party* assumes control of all or a part of the *business*?

The definition of “sell,” “selling,” “sale,” and “sold” in section 1798.140(t)(2)(D) addresses the issue, providing:

[A] business does not sell personal information when:

[¶] The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business provided that information is used or shared consistently with Section 1798.110 and 1798.115.

As part of its due diligence, the acquiring company should ascertain the target company’s compliance with the notice provisions of the CCPA and whether post acquisition, new notice should be provided if the acquiring company intends to use the *consumer person information* for a different or modified *business purpose*.

MISCELLANEOUS

The CCPA preempts local legislation “regarding the collection and sale of consumers’ personal information by a business.” (Civ. Code, § 1798.180.)

On or before January 1, 2020, the Attorney General is to solicit public participation to adopt regulations to further the purpose of CCPA. (Civ. Code, § 1798.185.)

The CCPA is to be construed liberally to effectuate its purpose. (Civ. Code, § 1798.194.)

The CCPA is operative January 1, 2020. (Civ. Code, § 1798.198(a).)