SPIRION
PROTECT WHAT MATTERS MOST

The California Consumer Privacy Act of 2018

The California Consumer Privacy Act of 2018 ("CCPA" or "the Act") became effective on January 1, 2020, and is codified at §§1798.100-199 of the Civil Code. The Act offers new and wide-ranging privacy rights for California residents, including a right to be informed about personal data collected by a business and rights to access and delete that information, a right to prevent personal information from being sold to third parties, and a right to data portability. The law applies to all business that collect or use this personal information, not just those companies operating in California. The California Attorney General may bring actions for civil penalties of up to $7,500 per violation and there is a limited private right of action for individual victims of data breaches for penalties ranging between $100-750 per violation.

CONTENTS

Sections

Key Issues

Note: These titles are unofficial descriptions.

In September of 2018, then-California Governor Jerry Brown signed into law S.B. 1121, which amended the CCPA by correcting grammatical and spelling errors, clarifying some aspects of the law, and making several substantive changes. Aspects that were clarified include:

- Information that nominally falls under one or more of the categories of "personal information" cited in §140(o)(A)-(K) is only personal information 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"
- The consumer private right of action only applies to violations of §150(a), which addresses security procedures and practices
- The Act does not apply if it is conflict to with the U.S. Constitution

Substantive changes include:

- Allowing a business to disclose the consumer's right to deletion of his/her personal information in a form that is "reasonably accessible to consumers"; previously, the Act required such information to be listed on a business's website or in its privacy policy
- Exempting personal information collected under the California Financial Information Privacy Act; this is in addition to personal information subject to the Gramm-Leach-Bliley Act, which was already exempt under the CCPA
- Exempting health care providers and covered entities "to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information" as it does under the Confidentiality of Medical Information Act (California's HIPAA analog) or under HIPAA

In October of 2019, California Governor Gavin Newsom signed into law several bills passed by the California legislature that address data protection and most of which were directed at the CCPA. Overall, the substance and strength of the Act remains the same but there are some additions and caveats that merit review by data protection professionals:

- A.B. 1202. Data brokers. Data brokers must now register with the California Attorney General's office.
- A.B. 25. CCPA amendment. One-year exemption for "employee" data.
- A.B. 874. CCPA amendment. Adds "reasonably" to the definition of "personal information."
- A.B. 1355. CCPA amendment. One-year exemption for "business-to-business" data; numerous drafting errors corrected.
- A.B. 1146. CCPA amendment. Exemption for certain information related to motor vehicle repairs and recalls.
- A.B. 1130. Breach notification. Adds new types of personal data subject to the state breach notification statute.

Below is an unofficial version of the Act that incorporates all previous amendments.

TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199]

(Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.)

1798.100.

(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(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. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(Amended by Stats. 2019, Ch. 757, Sec. 1. (AB 1355) Effective January 1, 2020.)

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.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

(Amended by Stats. 2019, Ch. 751, Sec. 1. (AB 1146) Effective January 1, 2020.)

1798.110.

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.
(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision

(a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about consumers.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.
(Amended by Stats. 2019, Ch. 757, Sec. 2. (AB 1355) Effective January 1, 2020.)

1798.115.

(a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer 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 pursuant to Section 1798.120.

(Amended by Stats. 2019, Ch. 757, Sec. 3. (AB 1355) Effective January 1, 2020.)

1798.120.

(a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

(d) A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

(Amended by Stats. 2019, Ch. 757, Sec. 4. (AB 1355) Effective January 1, 2020.)

1798.125.

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(b) (1) 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 a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision shall notify consumers of the financial incentives pursuant to Section 1798.130.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

(Amended by Stats. 2019, Ch. 757, Sec. 5. (AB 1355) Effective January 1, 2020.)

1798.130.

(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.
(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably

necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business' receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website and update that information at least

once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:
(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.
(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.
(Amended by Stats. 2019, Ch. 763, Sec. 1.3. (AB 25) Effective January 1, 2020.)

1798.135.

(a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:
(1) Provide a clear and conspicuous link on the business's 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 the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link

to the “Do Not Sell My Personal Information” Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers’ privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business’s privacy practices or the business’s compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer’s personal information, respect the consumer’s decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer’s personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer’s opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer’s personal information on the consumer’s behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer’s behalf, pursuant to regulations adopted by the Attorney General.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 8. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.140.

For purposes of this title:

(a) “Aggregate consumer information” means 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. “Aggregate consumer information” does not mean one or more individual consumer records that have been deidentified.

(b) “Biometric information” means an individual’s physiological, biological, or behavioral characteristics, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint,

can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) “Business” means:

(1) 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 collects consumers’ personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers’ personal information.

(2) Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. “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; or the power to exercise a controlling influence over the management of a company. “Common branding” means a shared name, servicemark, or trademark.

(d) “Business purpose” means the use of personal information for the business’s or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:
(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided that the personal information is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer’s experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(f) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "Consumer" means a 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.

(h) "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.
(4) Makes no attempt to reidentify the information.

(i) "Designated methods for submitting requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(j) "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

(k) “Health insurance information” means a consumer’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer’s application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) “Homepage” means the introductory page of an internet website and any internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application’s platform page or download page, a link within the application, such as from the application configuration, “About,” “Information,” or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.135, including, but not limited to, before downloading the application.

(m) “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(n) “Person” means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(o) (1) “Personal information” means information that identifies, relates to, describes, is reasonably 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 reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) 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, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
(E) Biometric information.

(F) 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 website, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) "Personal information" does not include publicly available information. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(p) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) "Research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(4) Subject to business processes that specifically prohibit reidentification of the information.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Not be used for any commercial purpose.

(9) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(t) (1) “Sell,” “selling,” “sale,” or “sold,” means 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 by the business to another business or a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer’s personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer’s personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135.
(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) 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 Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it

shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(u) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(v) "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.

(w) "Third party" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.
(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to

believe, that the person intends to commit such a violation.

(x) “Unique identifier” or “Unique personal identifier” means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, “family” means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.100, 1798.105, 1798.110, and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.
(Amended by Stats. 2019, Ch. 757, Sec. 7.5. (AB 1355) Effective January 1, 2020.)

1798.145.

(a) The obligations imposed on businesses by this title shall not restrict a business’ ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.
(6) Collect or sell a consumer’s personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer’s personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.
(2) For purposes of this subdivision, the definitions of “medical information” and “provider of health care” in Section 56.05 shall apply and the definitions of “business associate,” “covered entity,” and “protected health information” in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code and the information is not used, communicated, disclosed, or sold except as authorized by the Fair

Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) For purposes of this subdivision:

(A) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(B) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(h) (1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.
(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the

personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) “Contractor” means a natural person who provides any service to a business pursuant to a written contract.

(B) “Director” means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) “Medical staff member” means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) “Officer” means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) “Owner” means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.
(3) This subdivision shall not apply to subdivision (b) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2021.

(i) Notwithstanding a business’ obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or

refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(j) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

(k) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(l) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(m) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction 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 such company, partnership, sole proprietorship, non-profit, or government agency.

(2) For purposes of this subdivision:

(A) “Contractor” means a natural person who provides any service to a business pursuant to a written contract.

(B) “Director” means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) “Officer” means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) “Owner” means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2021.

(Amended by Stats. 2019, Ch. 763, Sec. 2.3. (AB 25) Effective January 1, 2020.)

1798.150.

(a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, 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:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. 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. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision

(a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

(Amended by Stats. 2019, Ch. 757, Sec. 9. (AB 1355) Effective January 1, 2020.)

1798.155.

(a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 12. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.160.

(a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature to offset any costs incurred by the state courts in connection with actions brought to enforce this title and any costs incurred by the Attorney General in carrying out the Attorney General's duties under this title.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with this title. These funds shall not be subject to appropriation or transfer by the Legislature for any other purpose, unless the Director of Finance determines that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with this title, in which case the Legislature may appropriate excess funds for other purposes.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.175.

This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section

22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.180.

This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative September 23, 2018, pursuant to Section 1798.199.)

1798.185.

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(4) Establishing rules and procedures for the following:
(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to Section 1798.120.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section

1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received from a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(b) The Attorney General may adopt additional regulations as follows:

(1) To establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household in order to address obstacles to implementation and privacy concerns.

(2) As necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.
(Amended by Stats. 2019, Ch. 757, Sec. 10. (AB 1355) Effective January 1, 2020.)

1798.190.

If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.
(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.192.

Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of

enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 14. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.194.

This title shall be liberally construed to effectuate its purposes.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.196.

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 15. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.198.

(a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 16. (SB 1121) Effective September 23, 2018.)

1798.199.

Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

(Added by Stats. 2018, Ch. 735, Sec. 17. (SB 1121) Effective September 23, 2018. Operative September 23, 2018.)

KEY ISSUE

Jurisdictional Thresholds

The Statute

The CCPA applies to any for-profit entity that conducts business in California and meets one or more of the following thresholds:

(1) Has annual gross revenue in excess of $25,000,000.

(2) Annually buys, receives, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices, alone, or in combination.

(3) Derives 50% or more of its annual revenue from selling consumers' personal information.

§1798.140(c).

An open question is whether the $25,000,000 threshold represents the business's gross revenue or is limited to those amounts generated by the business in California. Whether the statute applies extraterritorially is also an open question. Both of these questions are expected to be answered by the California Attorney General at some point. Note that for the second threshold, the 50,000 consumers/households/devices mark will be relatively easy to reach. A business could, e.g., receive the personal information of 20,000 individuals and their respective devices, requiring only 10,000 more instances of receipt to reach the overall threshold. Finally, start-up companies that publish mobile applications ("apps") and that collect and sell personal information as part of their business model will likely meet the third threshold relatively easily.

The Regulations

The Regulations do not change the jurisdictional scope of the statute or clarify it. They do give a definition of a "household," something missing from the statute: "'Household' means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier." §999.301(k). The Regulations also address the particulars for requests to access or delete household information. §999.318.

KEY ISSUE

Personal Information

The Statute

The CCPA uses a two-part definition of personal information, followed by a list of exemplar information types that qualify as "personal," assuming there is some linkage between the information in question and a California consumer:

> "Personal information" means information that identifies, relates to, describes, is reasonably 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 reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:
>
> A. 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, or other similar identifiers.
>
> B. Any categories of personal information described in subdivision (e) of Section 1798.80 [i.e., the state's secure records disposal statute].
>
> C. Characteristics of protected classifications [i.e., race, color, sex, etc.] under California or federal law.
>
> D. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
>
> E. Biometric information.
>
> F. 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 website, application, or advertisement.
>
> G. Geolocation data.
>
> H. Audio, electronic, visual, thermal, olfactory, or similar information.
>
> I. Professional or employment-related information.
>
> J. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

> K. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. [1]

The inclusion of "indirectly" in both parts of the definition means that information that is perhaps only tangentially linked to a person or is otherwise attenuated, such as geolocation information, is personal, and businesses that process that information are subject to the strictures of the Act. This greatly expands the scope of what qualifies as "personal."

The fact that the list of exemplars includes inferences made about other personal information on the list is particularly noteworthy; not even the EU General Data Protection Regulation's (GDPR) definition of personal data includes that. [2] Another difference between the CCPA and the GDPR approach to "personal" is that the latter has singled out some types of data as "special," such as data about race, ethnicity, religious beliefs, etc., that are included as "regular" personal information by the former.

Publicly available information, properly de-identified data, and aggregate consumer information are not considered personal information. [3]

The Regulations

The CCPA Regulations do not address the definition of personal information. With respect to personal information that is deidentified or in the aggregate the Regulations state that:

- A business may comply with a request to delete their personal information by "deidentifying the personal information" or "aggregating the consumer information." [4]
- "If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request." [5]

1. Cal. Civ. Code §1798.140(o).

2. However, the GDPR does proscribe profiling except under conditions; data subjects "have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Art. 22(1).

3. Cal. Civ. Code §1798.140(o)(2)-(3).

4. CCPA Regulations §999.313(d)(2)(b)-(c).

5. CCPA Regulations §999.323(f).

KEY ISSUE

Notices to Consumers

The Statute

The Statute contemplates that the California Attorney General will issue rules regarding the contents of notices to consumers, as well as their time of delivery, place, and manner. Section 1798.185 states, in pertinent part, that

> (a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:
> *
> *
> *
> (6) Establishing rules, procedures, and any exceptions necessary to ensure that **the notices and information that businesses are required to provide pursuant to this title** are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter. [emphasis added]

The Regulation

Article 2 of the Regulations addresses the providing of notices to consumers with respect to the use of their personal information. Section 999.305(a)(1) states that "[t]he purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them and the purposes for which the personal information will be used." Noteworthy about this notice requirement is the "plain English" mandate of §305(a)(2), which is part of a larger "user friendliness" theme of that section.

A business's use of personal information is circumscribed by the notice. In particular:

- A business shall not use a consumer's personal information for a purpose materially different than those disclosed in the notice at collection. If the business does wish to do so, it must go back to the consumer and obtain explicit consent for this new use. [1]
- A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection. [2]
- If a business does not give the notice at collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer. [3]

Contents of the notice include the following: [4]

- A list of the categories of personal information about consumers to be collected.
- For each category of personal information, the business or commercial purpose(s) for which it the categories of personal information will be used.
- If the business sells personal information, the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" (required by §999.315(a)), or in the case of offline notices, the web address for where the webpage to which it links can be found online.
- A link to the business's privacy policy, or in the case of offline notices, the web address of the where the business's privacy policy can be found online.

There are special rules for mobile devices [emphasis added]:

- The business may provide a link to the notice on the mobile application's download page and within the application. [5]
- When a business collects personal information from a consumer's mobile device for a purpose **that the consumer would not reasonably expect, it shall provide a just-in-time notice** (such as through a pop-up window) containing a summary of the categories of personal information being collected and a link to the full notice at collection. [6]
- A business shall post the notice of right to opt-out on the…the download or landing page of a mobile application. [7]
- The privacy policy shall be posted online through a conspicuous link using the word "privacy,"**…on the download or landing page of a mobile application**. …A mobile application may include a link to the privacy policy in the application's settings menu. [8]
- A business shall provide two or more designated methods for submitting requests to opt-out, **including an interactive webform** accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," **on the…mobile application.** [9]

1. CCPA Regulations §999.305(a)(5).

2. CCPA Regulations §999.305(a)(6).

3. Id.

4. CCPA Regulations §999.305(b)(1-4).

5. CCPA Regulations §999.305(b)(3).

6. CCPA Regulations §999.305(b)(4).

7. CCPA Regulations §999.306(b)(1).

8. CCPA Regulations §999.308(b).

9. CCPA Regulations §999.315(a).

KEY ISSUE

Privacy Policy

The Statute

Section 1798.130(a)(5) of the CCPA statute is the relevant section for a so-called privacy "policy" (in practice, a privacy statement for the consumption of people outside the organization). It states, pertinent part, that

> (a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:
> *
> *
> *
> (5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website and update that information at least once every 12 months:
>
> > A. A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.
> >
> > B. For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.
> >
> > C. For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:
> >
> > > i. A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.
> > >
> > > ii. A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

The Regulations

Section 999.308 of the CCPA Regulations develops the idea of a privacy policy. It states that "[t]he purpose of the privacy policy is to provide the consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information." Noteworthy about this privacy policy requirement is the "plain English" mandate of §308(a)(2), which is part of a larger "user friendliness" theme of that section.

Contents of the policy include: [1]
1) Right to know about personal information collected, disclosed, or sold;
2) Right to request deletion of personal information;
3) Right to opt-out of the sale of personal information;
4) Right to non-discrimination for the exercise of a consumer's privacy rights;
5) Authorized agent (i.e., how an authorized agent can make a request on the consumer's behalf);
6) Contact for more information;
7) Date the privacy policy was last updated;
8) If subject to the requirements set forth 999.317(g), which addresses record keeping by the business, the information compiled in section 999.317(g)(1), statistics on consumer requests for the previous calendar year, or a link to it; and
9) If the business has actual knowledge that it sells the personal information of minors under 16 years of age, a description of the processes required by sections 999.330 and 999.331, which describe how to opt into such sales.

- A list of consumer rights cited in §§1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, some examples of which include:
  - Consumer's right to request disclosure by a business of personal information collected
  - Consumer's right to request deletion by a business of personal information collected
  - Consumer's right to request disclosure by a business of personal information sold to third parties
- Personal information collected in the preceding 12 months by category;
- Personal information sold in the preceding 12 months by category;
- Personal information disclosed for a business purpose in the preceding 12 months by category.

1. CCPA Regulations §999.308(c).

KEY ISSUE

Consent

The Statute

Consent of a data subject to the proposed processing of his/her personal data is one of six possible legal bases for processing under Article 6 of the EU GDPR. Under the CCPA, however, consent plays a comparatively lessor role. There are three contexts under which consent applies under the CCPA statute:

- Under §1798.120(d), "[a] business that has received **direction from a consumer** not to sell the consumer's personal information or, in the case of a minor consumer's personal information **has not received consent** to sell the minor consumer's personal information shall be prohibited…from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides **express authorization** for the sale of the consumer's personal information."
- Under §1798.125(b)(3), "[a] business may enter a consumer into a financial incentive program only if the consumer **gives the business prior opt-in consent** pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, **and which may be revoked by the consumer** at any time."
- Under § 1798.105(d)(6), a business does not have to delete consumer personal information upon request if it is "[e]ngag[ing] in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, **if the consumer has provided informed consent.**"

[all emphasis added]

The Regulations

Consent features more prominently in the CCPA Regulations. Relevant citations include:

- §999.305(5). A business shall not use a consumer's personal information for purpose materially different than those disclosed in the notice at collection. If the business seeks to use a consumer's previously collected personal information for a purpose materially different than what was previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.
- §999.318. If a member of a household is a minor under the age of 13, a business must obtain verifiable parental consent before complying with a request to access specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 999.330.
- §999.330(a)(1). A business that has actual knowledge that it sells the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any

verifiable parental consent required under COPPA [i.e., the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501, et seq.].

[all emphasis added]

KEY ISSUE

Requests for Disclosure of Personal Information

The Statute

Per the CCPA statute §§1798.110 and 130, upon request, a business that holds personal information about a consumer must disclose within 45 days of a verifiable consumer request the following:

1. The categories of personal information it has collected about that consumer;
2. The categories of sources from which the personal information is collected;
3. The business or commercial purpose for collecting or selling personal information;
4. The categories of third parties with whom the business shares personal information; and
5. The specific pieces of personal information it has collected about that consumer.

The statute defines a "[v]erifiable consumer request" as a

> means a request that is made by a consumer…that the business can reasonably verify, pursuant to regulations adopted by the Attorney General…to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer…if the business cannot verify…that the consumer making the request is the consumer about whom the business has collected information…. [1]

The Regulations

The CCPA Regulations call this Request for Disclosure a "Request to Know":

> "Request to know" means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:
> 1. Specific pieces of personal information that a business has collected about the consumer;
> 2. Categories of personal information it has collected about the consumer;
> 3. Categories of sources from which the personal information is collected;
> 4. Categories of personal information that the business sold or disclosed for a business purpose about the consumer;
> 5. Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
> 6. The business or commercial purpose for collecting or selling personal information.

The Regulations provide specifics with respect to effectuating Requests to Know. Per §999.312, a business must provide 2 or more designated methods for a consumer to submit a Request to Know unless it's an online-only business and has a direct relationship with the consumer.

Per §999.313, businesses have

- 10 business days to confirm receipt of the Request to Know
- 45 calendar days to fulfil the Request to Know
  - Can extend 45 additional days but have to provide a reason within the first 45 days

[all emphasis added]

The in-scope time period runs 12 months prior to the date of the request.

Per §999.313, for requests that seek the disclosure of specific pieces of information about the consumer, if a business can't verify the identity of the person making the request, the business **shall not disclose any specific pieces of personal information** to the requestor and shall inform the consumer requestor that it cannot verify their identity. [2] [emphasis added]

Furthermore, "[a] business shall not disclose in response to a request to know a consumer's **Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers, or unique biometric data** generated from measurements or technical analysis of human characteristics." [3] [emphasis added]

However, the business shall (for example), respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data. [4]

---

1. Cal. Civ. Code §1798.140(y).

2. The CCPA Regulations §999.313(c)(1).

3. The CCPA Regulations §999.313(c)(4).

4. Id.

KEY ISSUES

Requests for Deletion

The Statute

Per §1798.105(a) of the CCPA statute, "[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." However, (and in contrast to the approach in the GDPR) this is subject to multiple exceptions for both businesses and service providers:

> 1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
> 2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
> 3) Debug to identify and repair errors that impair existing intended functionality.
> 4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.
> 5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
> 6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
> 7)To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
> 8) Comply with a legal obligation.
> 9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

Some of these exceptions are to be expected, given the nature of a relationship between the consumer and the business or service provider. Examples include the necessity to complete an underlying transaction between/among the parties or to comply with legal obligations. Others are somewhat vague, such as the exception for "solely internal uses that are reasonably aligned with the expectations of the consumer" or for internal uses that are "compatible with the context in which the consumer provided the information." Applying these latter exceptions will almost certainly require clarification by the Attorney General.

The Regulations

The CCPA Regulations add some context for businesses responding to a request to delete:

- If a business cannot verify the identity of the requestor, the business may deny the request to delete.

The business shall inform the requestor that their identity cannot be verified. [1]

- A business shall comply with a consumer's request to delete their personal information by:
  1. Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems [however, when the backup or achieve is restored or becomes active, the business must then erase];
  2. Deidentifying the personal information; or
  3. Aggregating the consumer information. [2]

One additional noteworthy mandate from the Regulation is the following:

- When a business denies a consumer's request to delete the business shall do all of the following:
  - Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law;
  - Delete the consumer's personal information that is not subject to the exception; and
  - Not use the consumer's personal information retained for any other purpose than provided for by that exception.

1. The CCPA Regulations §999.313(d)(1).

2. The CCPA Regulations §999.313(d)(2).

KEY ISSUE

Verification of Requestors

Verification Under the CCPA Statute

A leading challenge to a business in complying with the CCPA is determining whether a consumer who is requesting to know what information that business has on him/her is, in fact, truly that consumer and not an imposter. Section 1798.140(y) of the statute defines a "[v]erifiable consumer request" as "a request that is made by a consumer…that the business can reasonably verify…to be the consumer about whom the business has collected personal information." It goes on to state that "[a] business is not obligated to provide information to the consumer…if the business cannot verify…that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf." The statute cites a long list of requirements in the context of verification:

- A business shall provide the information specified in §1798.100(a) [i.e., the categories and specific pieces of personal information the business has collected] to a consumer only upon receipt of a verifiable consumer request. [1]
- A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to §1798.105(a) [i.e., right to request that a business delete any personal information about the consumer which the business has collected from the consumer] shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records. [2]
- A business that collects personal information about a consumer shall disclose to the consumer, pursuant to §1798.130(a)(3) [i.e., a business shall, in a form that is reasonably accessible to consumers the category or categories the personal information collected about the consumer in the preceding 12 months], the information specified in §1798.110(a) [i.e., what personal information is being collected and circumstances surrounding that collection] upon receipt of a verifiable consumer request from the consumer. [3]
- A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to §1798.130(a)(4) [i.e., information sold or disclosed in the previous 12 months], the information specified in 1798.115(a) [i.e., the categories of personal information collected, sold, and shared] to the consumer upon receipt of a verifiable consumer request from the consumer. [4]
- A business must disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. [5]
- The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' duty to disclose and deliver the information within 45 days of receipt of the consumer's request." [6]
- The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. [7]

Verification Under the CCPA Regulations

Section 999.323(a) of the Regulations prescribes the general rule of verification of the identity of requestors:

"A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information."

The rest of §999.323 addresses the process for constructing an identity verification process. Relevant points include:

- "Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section." [8] The concept of a third-party identity verification service is not found in the CCPA statute but is introduced here.
- "Avoid collecting the types of personal information identified in Civil Code section 1798.81.5(d), unless necessary for the purpose of verifying the consumer." This is a reference to personal information such as Social Security numbers, driver's license numbers and similar identification numbers, and other personal information that is particularly sensitive or advances identity theft. [9]
- Considerations of potential elements for use in the verification process include: [10]
  a. The type, sensitivity, and value of the personal information collected and maintained about the consumer (this point cites §1798.81.5(d) personal information as presumptively sensitive);
  b. The risk of harm to the consumer posed by any unauthorized access or deletion;
  c. The likelihood that fraudulent or malicious actors would seek the personal information;
  d. Whether the personal information to be provided by the consumer…is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;
  e. The manner in which the business interacts with the consumer; and
  f. Available technology for verification.

  Point "d" does not describe what qualifies as "robust"; the idea of certain types of personal information not lending itself to fraudulent requests is almost certainly new.

- A side effect of verifying a requestor is the necessity of asking him/her for additional personal information in order to complete the verification. Section 999.323(c) articulates the general rule that "[a] business shall generally avoid requesting additional information from the consumer for purposes of verification." It qualifies this by stating that

  [i]f, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes.

  This subsection closes by stating that "[t]he business shall delete any new personal information

collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317" [i.e., record keeping provisions].

- "A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to know or request to delete." [11]
- "If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request." [12]

1. Cal. Civ. Code §1798.100(c).
2. Cal. Civ. Code §1798.105(c).
3. Cal. Civ. Code §1798.110(b).
4. Cal. Civ. Code §1798.115(b).
5. Cal. Civ. Code §1798.130(a)(2).
6. Id.
7. Id.
8. The CCPA Regulations §999.323(b)(1).
9. The CCPA Regulations §999.323(b)(2).
10. The CCPA Regulations §999.323(b)(3).
11. The CCPA Regulations §999.323(d).
12. The CCPA Regulations §999.323(f).

KEY ISSUE

Sales to Third Parties

The Statute

Under §1798.140(w), the CCPA describes a third party as "a recipient of personal information who is not the business that collected it nor an entity operating on behalf of that business based on a contract [i.e., a service provider]." [emphasis added] This raises the question of what qualifies as a "sale." The definition of a sale under the CCPA is rather broad under §1798.140(t)(1):

> Sale. 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 by the business to another business or a third party for monetary or other valuable consideration.

In many cases a business may not realize that such a transfer is taking place. For example, a transfer of information to advertisers via cookies or advertising identifiers (for those clicking on advertisements) or a transfer of browser information to an analytics firm are likely sales under the CCPA.

Consumers have three rights with respect to sales of their personal data to third parties:

- A consumer can direct a business not to sell the consumer's personal information. [1]
- A business shall provide notice to consumers that their personal information may be sold to third parties and that consumers have the right to opt out. [2]
- A third party shall not sell personal information about a consumer unless the consumer has received explicit notice and is provided an opportunity to opt out. [3]

Note that for sale of the personal information of consumers under the age of 16, there is a requirement to "opt-in," either by the consumer or his/her parent or guardian. [4]

The Regulations

The CCPA Regulations do not expand upon the mandates set forth in the statute with respect to sales to third parties. One noteworthy area, however, is with respect to so-called "Do Not Track" mechanisms in web browsers that purport to tell advertisers not to process the personal data of a web users. The Regulations state that

> [i]f a business collects personal information from consumers online, **the business shall treat user-enabled global privacy controls**, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to **opt-out of the sale of their personal information as a valid request [to opt out of such a sale]…for the consumer**[.]" [5] [emphasis added]

As a result, a business that sells personal information to third parties would should have an automated

means to pass on the state of a Do Not Track signal to those third parties as part of its data protection compliance program. Moreover, third party purchasers of personal information will likely wish to mandate such communication in order to advance their own compliance.

1. Cal. Civ. Code §1798.140(v).

2. Cal. Civ. Code §1798.140(t)(2)(C).

3. The CCPA Regulations §999.314(a).

4. The CCPA Regulations §999.314(b).

5. The CCPA Regulations §999.314(c).

KEY ISSUE

Service Providers

The Statute

One area where the CCPA diverges from the GDPR is in the treatment of service providers (called "data processers" by the GDPR). The former cites relatively few mandates to service providers, while the latter devotes much of Chapter IV to regulation of processors, especially Article 28. The CCPA statute defines a service provider as "[a]n entity 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." [1] While any transfer of consumer personal information to another party in exchange for anything of value will almost certainly constitute a sale, the CCPA provides an exception for putative service providers if they meet certain criteria: [2]

(i) The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135 [i.e., a link to a Do Not Sell My Personal Information web page and a description of a consumer's rights listed in §1798.120, such as the right to opt-out of a sale of his/her personal information].

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

The Regulations

The CCPA Regulations add some context to the relationship between businesses and service providers and, while not regulating service providers to the same extend the GDPR regulates data processers, do add some considerations when businesses engage such entities:

- Businesses that provide services to non-profits or government agencies will be deemed service providers if they otherwise meet the definition: "A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations." [3]

- A business that is contracted by another business to gather personal information shall be deemed a service provider if it otherwise meets the definition of one: " To the extent that a business directs a second business to collect personal information directly from a consumer, or about a consumer, on the first business's behalf, and the second business would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations the second business shall be deemed a service provider of the first business for purposes of the CCPA and these regulations." [4]

- Service providers are proscribed from retaining, using, or disclosing personal information obtained in

the course of their providing services to a business. Five exceptions apply: [5]

1. *Cal. Civ. Code §1798.140(v).*
2. *Cal. Civ. Code §1798.140(t)(2)(C).*
3. *The CCPA Regulations §999.314(a).*
4. *The CCPA Regulations §999.314(b).*
5. *The CCPA Regulations §999.314(c).*

KEY ISSUE

Marketing and Advertising

The Statute

In contrast to Article 21(2) and (3) of the GDPR, there is no per se right to opt-out of advertising or marketing under the CCPA. However, the right to opt-out of sales of personal information under §§1798.120(a) and (b) and under §1798.115(d) effectively creates such a right. California consumers will likely face challenges with entirely opting out of the use of their personal data in the context of marketing and advertising. This is so owing to the web of relationships among companies that process personal information connected to Internet marketing and advertising – in many, if not most cases, a business will not necessarily know all of those companies.

Also in contrast to the GDPR and other EU law [1], browser cookies do not require any special considerations by businesses; they, along with web "beacons," advertising identifiers, and other technology related to advertising or marketing are all a species of "unique identifier" or "unique personal identifier," defined by §1798.140(x) as a

> means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

The closest analog in the GDPR to such identifiers is located in Recital 30, which states that

> [n]atural persons may be associated with **online identifiers provided by their devices, applications, tools and protocols**, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them. [emphasis added]

The Regulations

The CCPA Regulations also do not offer any additional consideration for cookies or other unique identifiers. It does cite unique identifiers in its definition of a "household," stating that "'[h]ousehold' means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier." [2] [emphasis added]

1. EU Directive 2009/136/EC, the EU "cookie law," extensively regulates the use of cookies.

2. The CCPA Regulations §999.301(k).

KEY ISSUE

Sales of Minors' Information

The Statute

In contrast to the opportunity given to California consumers to opt-out of the sale of their personal information, consumers who are minors must opt-in for such sale. Section 1798.120(c) of the CCPA statute establishes a 2-tier structure for determining who must give consent:

- Minors under 13 years of age. A parent or guardian must affirmatively authorize the sale.
- Minors 13-16 years of age. The minor can authorize the sale.

Note that this authorization structure applies to a business only if it "has actual knowledge that the consumer is less than 16 years of age" but that "[a] business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.[1]" This "actual knowledge" requirement is also cited in the CCPA Regulations.

The Regulations

Section § 999.330 of the CCPA Regulations addresses particulars of the opt-in process:

- Verifying the authorizing parent or guardian. A business must have a process in place to verify that the parent or guardian authorizing the sale of a minor's personal information is who they say they are: "A business that has actual knowledge that it sells the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under COPPA [i.e. the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501, et seq]." [emphasis added]
- Options for verification. The Regulation offers multiple options for verifying the putative parent or guardian:
  - Providing a consent form to be signed physically or electronically…under penalty of perjury[];
  - Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
  - Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
  - Having a parent or guardian connect to trained personnel via video-conference;
  - Having a parent or guardian communicate in person with trained personnel; and
  - Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information[ ].
- Verification in the context of a request to know or to delete. The options cited above for verification also apply when a parent or guardian executes a request to know or to delete on behalf of the minor: "A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth…[above]…for determining whether that a person submitting a request to

know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that child."

- Notice requirements to the parent or guardian. A business must provide notice to a parent or guardian opting-in how to later opt-out: "When a business receives an affirmative authorization pursuant to…[this regulation]…the business shall inform the parent or guardian of the right to opt-out and of the process for doing so on behalf of their child pursuant to section 999.315(a)-(f) [i.e., the specifics regarding the opt-out process applicable to all consumers]."

1. Cal. Civ. Code §1798.120(c).

KEY ISSUE

Financial Incentives

The Statute

The CCPA section 1798.125 cites the concept of a "financial incentive" in the context of (and as a foil to) "discrimination" against consumers for exercising any of the consumer's rights under the statute. Section 1798.125(a)(1) cites the following as examples of such discriminatory actions:

A. Denying goods or services to the consumer.
B. Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
C. Providing a different level or quality of goods or services to the consumer.
D. Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

However, this section qualifies the prospect of discrimination by stating that "[n]othing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data." [1]

There are two types of financial incentives, direct payments and differences in price, rate, level, or quality of goods/services. The statute states that

> [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 a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data. [2]

Other requirements of the statute:

- A business that offers any financial incentives pursuant to this subdivision shall notify consumers of the financial incentives pursuant to Section 1798.130 [i.e., consumer submission of requests for information]. [3]
- A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. [4]

The statute does not delve into any detail on how to calculate the value of a consumer's personal information; rather, it looks to the California Attorney General to promulgate the rules concerning this via the Regulations.

The Regulations

The CCPA Regulations define financial incentive as "a program, benefit, or other offering, including payments to consumers, related to as compensation, for the collection, retention disclosure, deletion, or sale of personal information." [5] As with the statute, the Regulations use the prospect of discrimination against a consumer as a foil, stating that "[i]f a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference." [6] This restriction is cited in Article 6 of the Regulations, the Article that addresses discriminatory practices.

With respect to the notice of the financial incentives, the Regulations explain that "[t]he purpose of the notice of financial incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision on whether to participate." [7] The Regulations note that if the business does not offer such an incentive, then no notice is required. [8]

The principles for the formatting of the notice are very similar that that of the privacy policy, namely: [9]

- Use plain, straightforward language and avoid technical or legal jargon;
- Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable;
- Be available in the languages in which the business provides contracts, disclaimers, sale announcements, and other information;
- Be reasonably accessible to consumers with disabilities; and
- Be readily available where consumers will encounter it before opting into the financial incentive or price or service difference.

Contents of the notice include the following: [10]

1) A succinct summary of the financial incentive or price or service difference offered;
2) A description of the material terms of the financial incentive or price or service difference;
3) How the consumer can opt-in to the financial incentive or price or service difference;
4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data.

With respect to calculating the value of consumer data, the Regulations state that "a business offering a financial incentive or price or service difference shall use and document a reasonable and good faith method for calculating the value of the consumer's data." [11] It offers the following as potential components of such a calculation: [12]

1) The marginal value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;
2) The average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;

3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers;
4) Revenue generated by the business from sale, collection, or retention of consumers' personal information;
5) Expenses related to the sale, collection, or retention of consumers' personal information;
6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference;
7) Profit generated by the business from sale, collection, or retention of consumers' personal information; and
8) Any other practical and reasonably reliable method of calculation used in good-faith.

Finally, in the event that a consumer uses a global privacy control (such as a Do Not Track browser signal) when participating in business's financial incentive program, the control will take precedence:

> If a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the **business shall respect the global privacy control** but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program. [13] [emphasis added]

1. Cal. Civ. Code §1798.125(a)(2).
2. Cal. Civ. Code §1798.125(b)(1).
3. Cal. Civ. Code §1798.125(b)(2).
4. Cal. Civ. Code §1798.125(b)(3).
5. The CCPA Regulations §999.301(j).
6. The CCPA Regulations §999.336(b).
7. The CCPA Regulations §999.307(a)(1).
8. Id.
9. The CCPA Regulations §999.307(a)(2).
10. The CCPA Regulations §999.307(b)(1)-(5).
11. The CCPA Regulations §999.337(a).
12. The CCPA Regulations §999.337(a)(1-8).
13. The CCPA Regulations §999.315(d)(2).

KEY ISSUE

Information Security

Information Security Under the CCPA Statute

The CCPA is not, per se, an information security or breach notification statute. California has distinct breach notification and information security statutes (§§1798.82 and 1798.81.5 of the Civil Code, respectively), both of which predate passage of the CCPA. Section 1798.150 represents the CCPA's requirements for protecting personal information using reasonable security procedures. Noteworthy about this section is that it couches the mandate in the negative, i.e., that the violation of the duty to protect personal information exposes the offending business to a civil action by the victim. The relevant text of §150(a)(1) reads:

> Any consumer whose nonencrypted and 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:
>
> A. To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> B. Injunctive or declaratory relief.
> C. Any other relief the court deems proper.
> [emphasis added]

If plaintiffs wish to pursue statutory damages, they must give 30 days' notice so the defendant can "cure" the breach; otherwise, they can go directly to court.
With respect to the cure of a breach, there is no guidance provided by the CCPA statute or the Regulations. What is known is that fixing the problem that caused the breach does not cure it; the offending entity must put the victim in the position they were before the breach. [1]

Information Security Under the CCPA Regulations

The CCPA Regulations provide insight into two related, if not overlapping, areas of information security: verification of requestors and implementation of controls to protect personal information. Section 999.313, Responding to Requests to Know and Requests to Delete, prescribes the following with respect to requests to know in the context of information security:

> c) Responding to Requests to Know
>
> 3) A business shall not provide a consumer with specific pieces of personal information **if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks.**
>
> *

*

*

6) A business **shall use reasonable security measures** when transmitting personal information to the consumer.

[emphasis added]

Section 999.323 presents General Rules Regarding Verification, some of which include:

a) A business shall establish, document, and comply with a **reasonable method for verifying** that the person making a request to know or a request to delete is the consumer about whom the business has collected information.

b) In determining the method by which the business will verify the consumer's identity, the business shall:

1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

*

*

*

d) A business **shall implement reasonable security measures** to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.

[emphasis added]

The Regulations prescribe a two-track system for verifying the identity of a requestor: one for requestors with an existing password-protected account and one for everyone else. Within this latter track are two standards, a base one if the requestor desires to know the categories of information collected and a higher one if the requestor desires to know the specific pieces of information collected. Section 999.324, Verification for Password-Protected Accounts, states in pertinent part the following:

a) If a business maintains a password-protected account with the consumer, the business **may verify the consumer's identity through the business's existing authentication** practices for the consumer's account[.]

b) **If a business suspects fraudulent or malicious activity** on or from the password-protected account, **the business shall not comply** with a consumer's request to know or request to delete **until further verification procedures determine that the consumer request is authentic**[.]

[emphasis added]

Section 999.325, Verification for Non-Accountholders, states in pertinent part the following:

a) If a consumer does not have or cannot access a password-protected account with the business, the business shall comply with this section, in addition to section 999.323.

b) A business's compliance with a **request to know categories** of personal information requires

> that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include **matching at least two data points provided by the consumer with data points maintained by the business**, ….
>
> c) A business's compliance with a request to know **specific pieces of personal information** requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, **which is a higher bar for verification**. A reasonably high degree of certainty may **include matching at least three pieces of personal information** provided by the consumer with personal information maintained by the business **…with a signed declaration under penalty of perjury** that the requestor is the consumer whose personal information is the subject of the request.
>
> d) A business's compliance with a **request to delete** may require that the business **verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity** of the personal information and **the risk of harm** to the consumer posed by unauthorized deletion.
>
> e) Illustrative scenarios follow [deleted]:
>
> f) If there is **no reasonable method** by which a **business can verify** the identity of the consumer to the degree of certainty required by this section, the **business shall state so in response to any request** and, if this is the case for all consumers whose personal information the business holds, **in the business's privacy policy** [i.e., their privacy notice].
> [emphasis added]

In sum, the responsibility to protect the confidentiality, integrity, and availability of consumer personal information is articulated in the context of (1) verifying that a requestor is who they say they are (i.e., protecting confidentiality) and (2) employing "reasonable security procedures and practices" to protect the integrity and availability of that information. In 2016, the California Attorney General's office published a report on data breaches that occurred during the period of 2012-2015. Among the recommendations made by the Attorney General is that

> [t]he 20 controls in the Center for Internet Security's Critical Security Controls identify a **minimum level of information security** that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment **constitutes a lack of reasonable security.** [2]

Citations to the report by the current California Attorney General are noteworthy by their absence, and it is unclear as to whether businesses should invest in advancing compliance using the Critical Security Controls.

Finally, the statute's requirement that the procedures and practices be "appropriate to the nature of the information" implies that a business must first conduct a risk assessment to understand the potential

for harm that could result from the exposure of that information, or from its destruction or damage to its integrity. The lack of such an assessment could expose the business to charges of not understanding the scope of the risk to personal information in its care.

1. See Romero v. Dep't Stores Nat'l Bank, 725 F. App'x 537, 540 (9th Cir. 2018).

2. California Data Breach Report 2012-2015, Kamala D. Harris, Attorney General, California Department of Justice (2016), at v.

KEY ISSUE

Enforcement

The Statute

California's Department of Justice, headed by the state's Attorney General, is the primary enforcer of compliance with the CCPA. Given that the office of the Attorney General is an elected position, the approach to CCPA policy making and enforcement may shift over time.

The Attorney General can seek fines of up to $2,500 per non-intentional violation and up to $7,500 per violation for intentional violations of the CCPA. [1] "Per violation" can be understood as per consumer. The Attorney General will give a business a 30-day notice to "cure" compliance violations before initiating a lawsuit. [2] However, this window of time may not be enough to make major changes to a privacy and security program or to implement a new one. In addition, the statute does not state what activities or outcomes qualify as "curing" a violation.

The CCPA also contains a narrow private right of action that will allow California consumers to bring lawsuits, including class action suits, against companies that have suffered a data breach where that business's own inadequate security practices exposed the personal information of those consumers. Section 1798.150(a)(1) states that

> [a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, 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:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
>
> (B) Injunctive or declaratory relief.
>
> (C) Any other relief the court deems proper.

Actions brought pursuant to this section require the consumer to "provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated." [3] Note that this requirement does not apply if the consumer initiates "an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title." [4]

The Regulations

The Regulations do not expand on or clarify issues related to enforcement or the private right of action,

such as the nature of a “cure” for a violation of the statute or what qualifies as “reasonable security procedures and practices.” There is one tangential reference to providing record keeping information to the Attorney General, upon request. [5]

1. Cal. Civ. Code §1798.155(b).

2. Id.

3. Cal. Civ. Code 1798.150(b).

4. Id.