TOP 5

Operational Impacts of the California Consumer Privacy Act

REVISED EDITION

The IAPP Westin Research Center

iapp
iapp.org

The Top 5 Operational Impacts of the California Consumer Privacy Act

The California Consumer Privacy Act was conceived and born in record time — not exactly "two days," as the story goes, but close — resulting in a comprehensive consumer privacy law that occasionally suffers from redundancy, drafting errors and lack of clarity. This e-book is intended to help privacy professionals make operational sense of the law as it takes effect and becomes enforceable in 2020.

The chapters that follow begin with the most basic of questions — "Do I fall under the law's scope?" — and then move through a variety of operational obligations, from transparency to fulfilling access and erasure requests to avoiding enforcement actions by the California attorney general.

As we wrote these pieces, we tried to focus as much as possible on those aspects of the law most likely to change the way you think about your privacy program. What new systems might you need to install? Where might you need more personnel? What new risk do you need to account for? We have based the organization on our successful e-books "Top 10 Operational Impacts of the GDPR" and "Top 10 Operational Responses to the GDPR" e-books that have now been downloaded more than 100,000 times from iapp.org, and we hope you find this e-book similarly useful.

As always, this work is based on our own research, crowd-sourced information from our surveys of members and, importantly, interviews with leading experts on the CCPA. Hopefully, you will find information you can use to formulate practical, real-world responses to what is perhaps the most all-encompassing privacy regulation ever passed at the state level.

Table of Contents

Determining If You're a Business Collecting or Selling Consumers' Personal Information

The CCPA applies only to businesses. The threshold question of the law's scope, therefore, is to determine whether your organization meets the elements of the "business" definition.

The best place to start is with the elements of "business," defined in Section 1798.140(c)(1)(A-C), that are objective and relatively clear. Answers to at least one of the following three questions must be "yes" for your organization to fall under the law's scope; if all the answers are "no," the law does not apply:

- Do you have annual gross revenues in excess of $25,000,000?
- Do you annually buy, receive for commercial purposes, sell or share for commercial purposes the personal information of 50,000 or more consumers, households or devices?
- Do you derive 50% or more of your annual revenue from selling consumers' personal information?

Assuming at least one of these is true, your organization is considered a business if all the following are also true:

- You are 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 your shareholders or other owners.
- You collect consumers' personal information, or someone collects it on your behalf.
- You alone or jointly with others determine the purposes and means of the processing of consumers' personal information.
- You do business in California.

The phrase "does business in California" is not defined in the CCPA. Instead, we reference the definition of "consumer" — a natural person who is a California resident — so the law applies to any business, whether or not geographically located in California, that collects and/or sells the personal information of California residents. This would be consistent with California's tax and corporations' codes, which apply broadly when a company engages in a transaction in California for purposes of financial gain or enters into repeated or successive transactions in California and its extensive long-arm jurisdiction law for civil litigation.

Do you "collect" and/or "sell" information?

Consumers have many new rights under the CCPA. These may be enforced against businesses that: (a) collect a consumer's personal information; (b) collect personal information about a consumer or about consumers; (c) sell consumers' personal information or disclose it for a business purpose; (d) sell personal information about a consumer to a third party; and/or (e) sell consumers' personal information to third parties.

A business is considered to "collect" personal information if it buys, rents, gathers, obtains, receives or even accesses it, by any means, whether actively or passively, including by observing a consumer's behavior. This definition is clearly intended to extend to online monitoring and tracking; it is broad in similar fashion to, for example, the EU General Data Protection Regulation's definition of "process."

"Selling" consumer personal information takes place upon "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means" for "monetary or other valuable consideration." The definition contains exclusions for consumer consent; conveying a consumer's opt-out instructions to a third party; or data transfers in the course of mergers, acquisitions, bankruptcies and the like.

Operationally, privacy professionals disclosing personal information to a service provider for a business purpose will want to ensure their contract restricts the service provider in its use or sale of the personal information.

"Selling" also excludes use for a business purpose, defined as using personal information for the operational purposes of the business or its service provider, so long as "reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed" or for another compatible operational purpose. The CCPA lists seven specific "business purposes" that include such things as counting ad impressions; detecting security incidents; debugging and repairing functionality; short-term "transient use" that isn't used for profiling; performing services on a business's behalf, such as fulfilling orders or processing payment (classic "data processor" activities); undertaking internal research for technological development; and "undertaking activities to verify or maintain the quality or safety" of the business's service or device.

Operationally, privacy professionals disclosing personal information to a service provider for a business purpose will want to ensure their contract restricts the service provider in its use or sale of the personal information. Under Section 1798.145, a business is not liable for the service provider's violation of the CCPA 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." Service providers are "likewise" not liable for the business's violation (presumably, of which they are not aware).

Although not clearly an exclusion to the law's scope, moreover, many consumers' rights conveyed under the CCPA would not apply to any business that only collects personal information for a "single, one-time transaction," provided the business doesn't sell the information, retain it or use it to "reidentify or otherwise link information" to the consumer.

Is it "personal information" under the CCPA?

Privacy professionals accustomed to thinking of personal information as personally identifiable information under U.S. state data breach laws will find the CCPA's definition of personal information far broader than usual. Those who have acclimated to the definition of "personal data" under the GDPR will not be as surprised.

Personal information is defined in Section 1798.140(o)(1) as "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." It includes information typically considered PII under state breach laws — names, unique personal identifiers, account names, Social Security numbers, driver's license numbers, passport numbers, biometric information and "other similar identifiers." But it also includes — to the extent it "identifies, relates to, describes, is reasonably capable of being associated with or could be reasonably linked to a consumer or household" — many other types of information, including aliases, IP addresses, "characteristics of protected classifications under California or federal law," commercial information (defined to include personal property records or purchasing history), geolocation data, internet activity (including browsing and search history, as well as web tracking data), professional and employment information, and education information. In addition, "personal information" includes "audio, electronic, visual, thermal, olfactory or similar information" and "inferences drawn" from any of the information contained in the definition.

The statute excludes from the definition publicly available information and "consumer information that is deidentified or aggregate consumer information." The term "deidentified" is defined as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked directly or indirectly to a consumer" and contains additional requirements.

The following are also excluded as "personal information":

- Protected health information that is collected by a covered entity or a business associate governed by the privacy, security and breach notification rules issued by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act. The law also excludes certain data from clinical trials.
- The sale of information to or from a consumer reporting agency for use in a consumer report consistent with the Fair Credit Reporting Act.
- Personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act, California Financial Information Privacy Act or Driver's Privacy Protection Act of 1994. That said, such exemptions do not apply to Section 1798.150 of the law, which addresses consumer rights to sue for data breaches.

Are your customers "consumers"?

Finally, and crucially, the law applies only if the business collects or sells personal information of consumers. The CCPA defines a "consumer" as a natural person — however identified, including by any unique identifier — who is a California resident.

The term "California resident" is defined in a separate California statute as:

- Every individual who is in California for other than a temporary or transitory purpose.
- Every individual domiciled in California who is outside the state for a temporary or transitory purpose.

Accordingly, if your business collects information from natural persons who live in California, even if they are traveling outside the state when they disclose their personal information, the law applies. That said, the CCPA's Section 1798.145 excludes a business from the law's scope, even if it collects or sells a consumer's personal information, "if every aspect of the commercial conduct takes place wholly outside of California." This occurs when: (1) the business collected the information while the consumer was outside of California; (2) no part of the sale of the consumer's personal information occurred in California; and (3) no personal information collected while the consumer was in California is sold. This section — confusing due to the contradictions between (1) and (3) — would apply if, for example, a California resident visits a single-source restaurant located outside of California. If, however, the California resident makes a reservation at the restaurant while still in California, that business is not excluded.

Importantly, the CCPA was amended in fall 2019 by Assembly Bill 25, which excludes from the law's coverage of personal information collected from people in their capacity as a job applicant or employee, at least until January 1, 2021.

Transparency and Notice Obligations

Among other things, the CCPA guarantees Californians the rights to know what personal information is being collected about them, to know whether their personal information is sold or disclosed and to whom, and to access their personal information. These rights create significant operational responsibilities.

In this chapter, we outline transparency obligations, but it can be a bit confusing and full of citations of the law. If you're inclined to get a more graphical representation of the information, see Appendix B.

Updating the privacy notice

The CCPA creates specific transparency obligations relating to collected and sold personal information. In particular, a business must disclose in its online privacy notice and in any California-specific description of consumers' privacy rights (or, if the business does not actually have a privacy notice, it still has to put the information somewhere on its website), the following, pursuant to Sections 1798.130(a)(5)(A) and 1798.105(b):

- A description of consumers' rights under Section 1798.110 to request:
    - The categories of personal information the business has collected about the consumer.
    - The categories of sources from which the personal information is collected.
    - The business or commercial purpose of collecting or selling personal information.
    - The categories of third parties with whom the business shares personal information.
    - The specific pieces of personal information the business has collected about the consumer.

- A description of consumers' rights under Section 1798.115 to request:
    - The categories of personal information the business collected about the consumer.
    - The categories of personal information the business sold about the consumer.
    - The categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.
    - The categories of personal information about the consumer that the business disclosed for a business purpose.
- A description of consumers' rights under Section 1798.125 not to be discriminated against for exercising any the CCPA rights.
- One or more designated means for consumers to submit requests, including (at minimum) a toll-free number. (In the case of a business that operates exclusively online and has a direct relationship with the consumer, only an email address for submitting requests is required.)
- The right to deletion of personal information.

Collectors of personal information

The CCPA defines "collectors" and "sellers" of consumers' personal information in Sections 1798.140(e) and (t)(1). While not all collectors are sellers, a seller is most likely a collector. The CCPA applies the obligations outlined below to all businesses that collect personal information.

Section 1798.130(a)(5)(A) does not make it clear whether businesses that collect but do not sell consumers' personal information

Section 1798.100(b) requires a business that collects a consumer's information to, "at or before the point of collection":

- Inform consumers of the categories of personal information to be collected.
- Inform consumers of the purposes for which the categories of personal information shall be used.
- Provide notice of the collection of any additional categories of information or use of collected information for any additional purposes taking place after initial disclosures have been made.

Section 1798.105(b) requires any business collecting personal information about consumers to "disclose … the consumer's rights to request deletion of the consumer's personal information." Operationally, businesses should make sure that disclosures of this right to request deletion also include its limitations, set forth in Section 1798.105(d). Those limitations consist of nine enumerated exemptions.

Section 1798.110(c) requires, "pursuant to Section 1798.130(a)(5)(B)," that a business that collects personal information about a consumer disclose:

- The categories of personal information it has collected about the consumer.
- The categories of sources from which the personal information is collected.
- The business or commercial purpose of collecting or selling personal information.
- The categories of third parties with whom the business shares personal information.
- The specific pieces of personal information the business has collected about the consumer.

Section 1798.110(c) is identical to Section 1798.110(a), which describes consumers' right to request information, with the addition of a reference to Section 1798.130(a)(5)(B), which clarifies that "the list of categories of personal information" that must be disclosed means categories of personal information collected by the business about consumers in the preceding 12 months, "by reference to the enumerated category or categories in Subdivision (c) of Section 1798.130 that most closely describe the personal information collected." Section 1798.130(c) likely refers to Section 1798.140's definition of personal information, which includes 11 enumerated subcategories.

Categories of personal information will be discussed further in part three of this series.

All disclosures must be "in a form that is reasonably accessible to consumers" and updated "at least once every 12 months." The use of the word "and" in Section 1798.130(a) may require identical disclosures in multiple written policies. Aside from the specific disclosures discussed above that must be included in a business's online privacy policy or California-specific description of rights, the statute is silent on the specifics of how disclosures must take place.

Transfers to third parties

Some businesses, in addition to acquiring information from or about consumers, also transmit that information onward. Businesses that sell personal information about consumers or disclose it "for a business purpose" are a subcategory of businesses that collect personal information and have additional disclosure obligations. Section 1798.115(c) and Section 1798.130(a)(5)(C), these businesses must release two specific lists:

- The category or categories of personal information sold in the last 12 months, or if information has not been sold in the preceding 12 months, that fact.
- The category or categories of personal information disclosed for a business purpose in the last 12 months, or if no such disclosure has occurred in the preceding 12 months, that fact.

Businesses that sell consumer information to third parties are further obligated, per Section 1798.120(b), to disclose that:

- Consumer information may be sold.
- Consumers have the right to opt out of the sale of their personal information.

Section 1798.135 adds that businesses who sell personal information must disclose the above information in a form readily accessible to consumers and:

- Provide a "clear and conspicuous" link on the business's homepage, titled "Do Not Sell My Personal Information."
- Not require consumers to create an account to direct the business not to sell their personal information.
- Include a description of the consumer's rights under Section 1798.120 and a separate link to the "Do Not Sell My Personal Information" page in:
    - Its online privacy policy or policies, if the business maintains them.
    - Any California-specific description of consumer privacy rights.

As mentioned above, businesses that sell personal information will need to comply with the obligations of those that collect personal information, as well.

Takeaways

Identifying what personal information a business has, where it comes from, where it is stored and where it is transferred are the first steps in complying with the CCPA's notice and transparency requirements. Without good data mapping and inventory, no business can hope to accurately make the category-centric disclosures emphasized by the statute, let alone comply with verified requests from consumers for specific pieces of personal information.

Without good data mapping and inventory, no business can hope to accurately make the category-centric disclosures emphasized by the statute

As both collectors and sellers of personal information are required to disclose the categories of information collected, based on the enumerated list located in Section 1798.140, all businesses covered by the CCPA should pay careful attention to any regulations ultimately adopted by the Office of the Attorney General of California under Section 1798.185(a)(1). The attorney general must "solicit broad public participation" on or before January 1, 2020, to adopt regulations that, among other things, will "[update] as needed additional categories of personal information to those enumerated" in Section 1798.130(c) and Section 1798.140(o) "in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns."

Businesses that sell or "transfer for a business purpose" should quickly ensure they have a complete inventory of all parties receiving their data. Businesses that do not sell data for cash but do transfer it to third parties may yet qualify as sellers; they should pay careful attention to the requirements that attach to "business purpose" transfers, including the duty to inform consumers when such transfers have not taken place.

Only after completing thorough data mapping and inventory should businesses begin updating privacy policies and California-specific rights pages and putting in place (if necessary) "Do Not Sell My Information" apparatus.

Responding to Consumers' Personal Information Access Requests

Consumers have long been entitled to transparency regarding businesses' privacy practices. But the CCPA for the first time gives consumers a right to request specific information about how their personal data is processed, for what purposes and with whom it is shared. The law also gives consumers the right to receive answers to these requests, free of charge, within 45 days, in an electronic format they can transfer to another business.

In this chapter, we address how businesses should prepare for consumers' personal information access requests. If you have followed the steps outlined in the first two chapters of this e-book — determining if you're a business collecting California consumers' personal information, conducting data inventory and mapping exercises, and updating privacy notices to comply with the law's transparency obligations at data collection — then building a system to respond to access requests will be a lighter lift.

Verifiable requests

As we learned last chapter, consumers' rights to request information about the processing, disclosure and/or sale of their personal information include being notified of this right in the public-facing privacy notice. As well, Section 1798.130(a) requires businesses to make available to consumers two or more designated methods for submitted access requests, including, "at a minimum," a toll-free telephone number and a website address. This latter requirement may involve submitting a form online or perhaps sending an email to a designated address made available on the business's website. The law was amended in fall 2019 to allow businesses that operate exclusively online and have a direct relationship with the consumer to offer an email address, rather than a phone number, for receiving consumer requests.

The consumer's request must be "verifiable," defined in Section 1798.140(y) as a request the consumer makes on their own behalf or that of their child that the business can "reasonably verify" pursuant to regulations the attorney general of California will adopt in the coming months. One authorized delivery mechanism for the response is via the consumer's account with the business, which may provide a means for verification via the consumer's unique login credentials. Businesses have the authority to determine which authentication measures are reasonable in light of the personal information requested but shall not require consumers to create an account to make a verifiable request. Pursuant to 1798.185, the attorney general may establish rules and procedures on how to comply with verifiable consumer requests.

Businesses that have built systems for receiving and even automatically responding to data subject access requests pursuant to the GDPR will likely have also developed means for authenticating the consumer's request.

Substantive response

Consumers' rights to request — and businesses' corresponding obligations to respond — are set forth in three separate sections of the CCPA, triggering slightly differing response obligations depending on the circumstances.

Business that collects a consumer's personal information

Pursuant to Section 1798.100(a), (b) and (c), a consumer has a right to request, and a business that "collects a consumer's personal information" has an obligation to disclose upon a verifiable request: (1) the categories of personal information the business has collected; and (2) the specific pieces of personal information the business has collected.

Business that collects personal information about a consumer

Pursuant to Section 1798.110(a) and (b), a consumer has a right to request, and a business that "collects personal information about a consumer" has an obligation to disclose upon a verifiable request: (1) the categories of personal information the business has collected about the consumer; (2) the specific pieces of personal information the business has collected; (3) the categories of sources from which the personal information was collected; (4) the business or commercial purpose for the collection; and (5) the categories of third parties with whom the business shares the personal information.

Businesses that have built systems for receiving and even automatically responding to data subject access requests pursuant to the GDPR will likely have also developed means for authenticating the consumer's request.

Business that sells a consumer's personal information or discloses it for a business purpose

Pursuant to Section 1798.115(a) and (b), a business that sells a consumer's personal information, discloses it for a business purpose or both is required to provide a consumer with the following information when they submit a verifiable request: (1) the categories of personal information it has collected about the consumer; (2) the categories of personal information it has sold about the consumer; (3) the categories of third parties to whom the personal information was sold (organized by category of personal information for each third party); and (4) the categories of personal information it disclosed about the consumer for a business purpose.

Categories of personal information

Some of the more confusing provisions in the statute are those specifying what belongs in the "categories of personal information" response, discussed in Section 1798.110 (collection about consumers) and Section 1798.115 (selling or disclosing for business purpose) responses in Section 1798.130(3) and (4). Those provisions reference "the enumerated category in Subdivision (c) that most closely describes the personal information" without clearly specifying which Subdivision (c). The most logical choice is Section 1798.130(c), which, in turn, references the statute's definitions section (1798.140), in which "personal information" is defined in Subsection (o) with 11 "categories" (a through k).

A business responding to a Section 1798.110 (collection about consumers) request must identify the category or categories of personal information collected about the consumer in the preceding 12 months by referencing the information defined in one of those sections. A business responding to a Section 1798.115 (selling or disclosure) request must: (1) identify the category(ies) that most closely describes the personal information sold, as well as the categories of third parties to whom it was sold, on one list; and (2) on a separate list (if applicable), do the same thing for personal information disclosed to third parties for a business purpose.

Response timing and methods

Although Section 1798.100(d) requires a business to disclose and deliver the personal information "promptly," more specific guidance may be found in Section 1798.130(a)(2), which also applies to consumer access requests under 1798.100, as well as .110 and .115. In short, responses should be:

- Free of charge.
- Delivered within 45 days of receiving the verifiable request (which may be extended by an additional 45 days "when reasonably necessary" or up to 90 additional days "where necessary" under Section 1798.145(g)(1) "taking into account the complexity and number of requests" and provided the consumer is notified within 45 days of the extension and its reasons).
- For the 12-month period preceding the access request.
- Made in writing, in a "readily usable format" that allows the consumer to transmit the information from one entity to another "without hindrance."
- Delivered through the consumer's account, by mail or electronically at the consumer's option.

Businesses may not require consumers to open an account just to receive their personal information report. They also may not extend the 45-day response period to accommodate a lengthy verification process.

Businesses are not obliged to respond to a consumer's requests more than twice in a 12-month period. In addition to having verification procedures, therefore, businesses will also want to track when access requests are received, when responses are sent and how often the same consumer requests her personal information. Of course, this may itself constitute "personal information" subject to disclosure.

Exceptions

The CCPA contemplates that in certain circumstances a business may elect not to respond substantively to the consumer's request for access to personal information. Pursuant to Section 1798.145(g), the business must inform the consumer: (1) of its reasons for not taking action; and (2) of any right to appeal that decision. The statute does not clearly give the consumer a right to appeal, but it appears the business might, especially to avoid an action under Section 1798.150(b)(1).

The CCPA also permits the business to either charge a fee or refuse to respond, upon notifying the consumer of its reasons, if the consumer's requests are "manifestly unfounded or excessive, particularly because of their repetitive character." The burden to demonstrate the request's character rests with the business.

Training

A final operational requirement — applicable not just to consumer access requests, but also to other aspects of consumers' privacy rights under the law — is to ensure that "all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with [the CCPA] are informed of all requirements" in the law's transparency and access request provisions. Pursuant to Section 1798.130(6), employees should also be trained in how to help consumers exercise their rights.

Rights of Erasure, Objection to Sale and Non-Discrimination

As we've already learned, the CCPA aims to ensure various individual rights. In this chapter, we discuss the right to erasure, ability to object to the sale of their personal information, and "right to opt out" and "right to opt in," all of which come with significant operational impacts.

Specifically, the "right to opt in" applies to consumers under the age of 16, requiring businesses to obtain their affirmative consent — or the affirmative consent of a parent or guardian — before selling any of these consumers' personal information.

In addition, the law also protects Californians' right "to equal service and price, even if they exercise their privacy rights," which presents additional operational requirements.

Right of erasure

The CCPA's Section 1798.105 grants consumers the right to request erasure of "any personal information about the consumer which the business has collected from the consumer." It requires businesses to fulfill such requests — and to direct "any service providers" to do the same — within 45 days of receiving a "verified request" or "verifiable request" from the consumer. A rights-disclosure provision also requires businesses that collect personal information about consumers to disclose to those consumers their rights to request the deletion of their personal information. Lastly, it carves out various exceptions to this right of erasure. If certain conditions are met, businesses may not be required to delete a customer's personal information upon receiving an erasure request.

Perhaps the most broadly worded exceptions concern "internal uses" of personal information. These exceptions, for example, will allow businesses to continue to use a consumer's personal information that has been the subject of an erasure request "internally, in a lawful manner that is compatible with the context in which the consumer provided the information." A similar exception is carved out for "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."

Another exception allows businesses that engage in "public or peer-reviewed … research in the public interest" to ignore erasure requests "when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research." However, two further conditions must be met before this exception may apply: First, the business must adhere to "all other applicable ethics and privacy laws," and second, the consumer must have provided "informed consent" for the conduct of the research.

Businesses are also not required to delete information "if it is necessary" to:

- Complete the transaction for which it was collected.
- Provide a good or service the consumer has requested.
- Perform a contract between the business and the consumer.
- Detect security incidents.
- Protect against "malicious, deceptive, fraudulent, or illegal" activities.
- Prosecute people responsible for "malicious, deceptive, fraudulent, or illegal" activities.
- "Debug to identify and repair errors that impair existing intended functionality."
- Ensure the exercise of free speech by another customer.
- Ensure the company's exercise of "another right provided for by law."
- Comply with a legal obligation, in particular, those of 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.

Businesses that sell personal information must provide consumers with "explicit notice" that they may sell their personal information to a third party.

Objection to sale

The CCPA provides for two related rights regarding the sale of personal information: a "right to opt out" in Section 1798.120 (a-c) and a "right to opt in" in Section 1798.120(d). The first authorizes consumers to opt out of the sale of their personal information by a business. That is, a consumer may direct a business not to sell its personal information. Moreover, businesses that sell personal information must provide consumers with "explicit notice" that they may sell their personal information to a third party, as well as "an opportunity to exercise the right to opt out" before any selling occurs. A consumer may exercise this right "at any time" and may also authorize another person to opt out on their behalf. Businesses that are directed by a consumer or their designee not to sell their personal information may not do so "unless the consumer subsequently provides express authorization" for such sale. Once a consumer has opted out of the sale of their personal information, a business must wait at least 12 months before requesting that the consumer authorize its sale. Finally, any information the consumer provides in connection with their opt-out request must be used "solely for the purposes of complying" with that request.

The right to opt in, meanwhile, requires businesses to obtain affirmative authorization from consumers between the ages of 13 and 16 and from the parent or guardian of consumers under the age of 13 before selling any of their personal information. The CCPA thus prohibits businesses from selling the personal information of a consumer they have "actual knowledge" is between the ages of 13 and 16, unless the consumer has "affirmatively authorized" the sale. Moreover, businesses are prohibited from selling the information of a consumer under the age of 13 unless they have obtained affirmative authorization from the consumer's parent or guardian. This section of the law also makes it clear that a business will be considered to have had actual knowledge of a consumer's age if it "willfully disregards" their age. Operationally, an important question is whether failing to ask for or require a consumer to provide proof of age at the point of sale constitutes willful disregard of it.

The "do not sell" button

To meet their obligations regarding the opt-in/-out rights enshrined in the CCPA within Section 1798.135, businesses must provide a "reasonably accessible" and "clear and conspicuous link" on their homepage, titled "Do Not Sell My Personal Information." This link must enable a consumer to opt out of the sale of their personal information but must not require them to create an account to do so. The link must also describe the consumer's rights pursuant to this section and must be contained in its online privacy policy or policies, as well as any "California-specific description of consumers' privacy rights" that it maintains.

Additionally, the homepage containing this link to the opt-out request need not be made available to the general public but only needs to be available to California consumers. That is, to comply with these obligations, businesses may maintain "a separate and additional homepage that is dedicated to California consumers and that includes the required links and text," as long as they have taken "reasonable steps" to ensure California consumers are directed to it.

Lastly, this section of the CCPA places obligations on businesses to ensure "individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title," for example, data protection officers, are informed of the relevant requirements and know how to direct consumers to exercise their rights.

Data broker registry

A closely related law passed in fall 2019, along with amendments to the CCPA (AB 1202), creates a requirement for data brokers to register with the attorney general. The law defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." This does not include consumer reporting agencies, financial institutions governed by the GLBA or entities covered by the Insurance Information and Privacy Protection Act. Under California Civil Code Section 1798.99.82, data brokers must pay a registration fee to the attorney general and provide certain information, including name, address and website address. Failure to register may result in a penalty of $100 per day, plus other costs. The law explicitly provides that it is not intended to interfere with or supersede the CCPA.

Non-discrimination

The CCPA also contains a non-discrimination provision in Section 1798.125 that relates to the prices and quality of goods and services a business provides to its consumers. To protect consumers who exercise their privacy rights under this law, the provision prohibits businesses from: (1) denying them goods or services; (2) charging them a different (i.e., higher) price; (3) providing them goods or services of a different (i.e., lower) quality; or (4) suggesting that (2) or (3) will occur. As the law states in a "complex and seemingly self-contradictory" exception, however, businesses may charge different prices or provide a different level or quality of goods or services to consumers that exercise their privacy rights "if the difference is reasonably related to value provided by the consumer's data."

As explained in the law, the bill thus "would authorize businesses to offer financial incentives for collection of personal information." Financial incentives would include, for example, "payments to consumers as compensation … for the collection … sale … or the deletion of personal information." Businesses that do offer financial incentives for the collection of consumers'

personal information must also notify consumers of these offers, and consumers must give businesses their "prior opt-in consent" to enter the program, which they may revoke "at any time." Lastly, these financial incentives and the practices surrounding them must not be "unjust, unreasonable, coercive, or usurious in nature."

In operational terms, the CCPA may prompt some businesses to specify the value of the personal data they collect from each consumer. This opens up numerous intriguing questions: How much is an email address worth? What about a phone number or home address? What is the relative value of other types of personal information that are mentioned in Section 1798.140, such as a person's "preferences, characteristics, psychological trends, … predispositions, behavior, attitudes, intelligence, abilities, and aptitudes"? If businesses do decide to offer financial incentives to customers to collect their personal information, it will be interesting to see how and by what means they price this information.

Penalties and Enforcement Mechanisms

In this chapter, we look at what happens if organizations that are in scope of the law fail to alter operations and are therefore not in compliance. Violating the CCPA exposes organizations to potentially large civil penalties and statutory damages. Thanks in part to these large fines, as well as California's size and population, the CCPA will heavily influence data protection practices nationwide.

Civil penalties under the CCPA and Section 17206 of the Business and Professions Code

The major liability section of the CCPA is found in Section 1798.155(a) of Title 1.81.5. Under Subsection (a) of this provision, California's attorney general is empowered to bring an action against any company or individual person violating the CCPA for up to $2,500 as allowed by Section 17206 of the Business and Professions Code. However, enterprises have 30 days after receiving notice of noncompliance from the California attorney general's office to cure it, and only thereafter are they subject to an enforcement action for violating the law. This system is the same as that used to enforce the California Online Privacy Protection Act, a 2003 law that required website operators to "conspicuously" post a privacy policy on their website if the site collects PII. It is likely that the enforcement of the CCPA will follow the same rules as CalOPPA and other similar laws that use Section 17206 for a penalty. This means damages will be tabulated on a per-capita basis. Each user whose profile is illegally processed, sold, etcetera, will represent an independent violation.

To illustrate, if a business sells the profiles of 100 users who have asked that their information not be sold, the maximum penalty is $25,000, not $2,500. This interpretation finds support in the 1973 California Supreme Court case People v. Superior Court, which held that the number of violations is the number of persons the violations were directed at, with multiple violations against the same person (in that case material misstatements) counted together as one violation. Therefore, the sale of one profile multiple times will likely constitute a single violation.

Damages calculations under Section 17206 may be mitigated if the defendant lacks the financial ability to pay the penalties as mitigation (see People v. First Federal Credit Corp. and Hewlett v. Squaw Valley Ski Corp.). Moreover, penalties are set under Section 17206(b) by considering the nature, persistence, length, willfulness and seriousness of the misconduct, such as when the California attorney general applied CalOPPA to mobile apps in 2012.

The CCPA does present one crucial difference from CalOPPA and its other predecessors: Intentional violations have a higher cap of $7,500, as specified in Section 1798.155(b). This indicates the California Legislature views willful violations of data privacy more seriously than unfair competition violations and may, if imposed to the full extent of the law, threaten to drive out of business enterprises that willfully violate the law.

To illustrate the implications of these penalties, consider its possible effect on Facebook, whose Cambridge Analytica scandal was one of the motivations for the citizen's initiative inspiring the CCPA (see Section 1798.198(b)). According to publicly available data and some estimation, Facebook has approximately 24.6 million users in California. Using this number, were Facebook found to have violated the CCPA, it could face a rough full maximum penalty of $61.6 billion for an unintentional violation affecting each of its users and up to $184.7 billion for an intentional violation.

The CCPA does present one crucial difference from CalOPPA and its other predecessors: Intentional violations have a higher cap of $7,500.

Private right of action under the CCPA

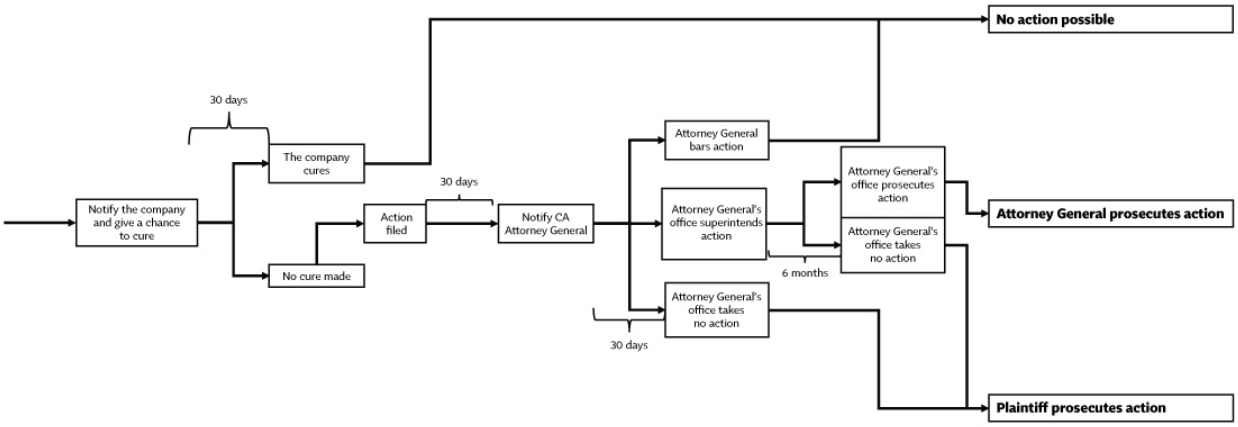
The CCPA, unlike CalOPPA, grants a private right of action to individual Californians under Section 1798.150 of Title 1.81.5. The section gives any natural person with California residency a right of action if their unencrypted or unredacted personal has been exposed due to a business's failure to maintain appropriate security safeguards. It should be noted the definition of personal information in this section is that defined in Title 1.81, Section 1798.81.5(d)(1)(A), not the definition found in the remainder of the act. This definition is sufficiently narrower and limited to a person's name (at least first initial and last name) and either their Social Security number, driver's license or state identification number, bank or credit card information, or medical or health insurance information.

There is no pecuniary damages requirement; plaintiffs can instead seek statutory damages between $100 and $750, injunctive or declaratory relief, or "any other relief the court deems proper." Actual damages are only recoverable if they exceed the statutory damages. Actions can be aggregated into a class action. The rejection of an actual damage requirement is consistent with a recent 9th Circuit decision earlier this year. The 9th Circuit found the risk of identity theft caused by a breach of personal information permits a federal action against the data controller, with no actual damages or specific evidence of identity theft required.

Although it doesn't have a pecuniary damages requirement, the private right of action has two checks. First, the action is subject to the same notice requirement as its public counterpart. Prospective plaintiffs, except those pursuing an individual action for pecuniary damages, must give a prospective defendant business written notice of the intended action and 30 days to cure the problem. The action can only proceed if the company fails to fix the problem within the time allotted.

Second, the California attorney general has the authority to stop or superintend a private action. Within 30 days of filing the action, after the chance to cure has elapsed, the plaintiff must notify the attorney general's office. The attorney general can decide to prosecute the action, instead of the customer, or bar the customer from proceeding with the action. If the office does not act within 30 days of receiving the notice or proceed with the action within six months of informing the putative plaintiff they intend to prosecute, the plaintiff may continue their action unimpeded.

Here is a flow chart of the full CCPA private action procedure:



The attorney general's ability to issue interpreting regulations

Under Section 1798.185 of Title 1.81.5, the California attorney general is authorized to promulgate regulations after public comment regarding more detailed implementation of the CCPA and additional regulations "as necessary to further the purposes of this title." This includes the categories of personal information covered, definitions of terms, exemptions needed for compliance with other laws, and rules and procedures for following the law. The attorney general has issued draft regulations and accepted public comments; the final regulations are expected to be issued before the law's July 1 enforcement deadline.

Appendix A

THE CALIFORNIA CONSUMER PRIVACY ACT

The Legislature finds and declares that:

(a) In 1972, California voters amended the California Constitution to include the right of privacy among the "inalienable" rights of all people. The amendment established a legal and enforceable right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.

(b) Since California voters approved the right of privacy, the California Legislature has adopted specific mechanisms to safeguard Californians' privacy, including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act and Shine the Light, a California law intended to give Californians the "who, what, where, and when" of how businesses handle consumers' personal information.

(c) At the same time, California is one of the world's leaders in the development of new technologies and related industries. Yet the proliferation of personal information has limited Californians' ability to properly protect and safeguard their privacy. It is almost impossible to apply for a job, raise a child, drive a car or make an appointment without sharing personal information.

(d) As the role of technology and data in the daily lives of consumers increases, there is an increase in the amount of personal information shared by consumers with businesses. California law has not kept pace with these developments and the personal privacy implications surrounding the collection, use and protection of personal information.

(e) Many businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer's personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks, to name a few categories.

(f) The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress and even potential physical harm.

(g) In March 2018, it came to light that tens of millions of people had their personal data misused by a data-mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the internet. As a result, our desire for privacy controls and transparency in data practices is heightened.

(h) People desire privacy and more control over their information. California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information. It is possible for businesses both to respect consumers' privacy and provide a high-level transparency to their business practices.

(i) Therefore, it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information by ensuring the following rights:

(1) The right of Californians to know what personal information is being collected about them.

(2) The right of Californians to know whether their personal information is sold or disclosed and to whom.

(3) The right of Californians to say no to the sale of personal information.

(4) The right of Californians to access their personal information.

(5) The right of Californians to equal service and price, even if they exercise their privacy rights.

TITLE 1.81.5. California Consumer Privacy Act [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 October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

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 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's 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 October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

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 October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.115.

(a) A consumer shall have the right to request that a business that sells the consumer's personal information or 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 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 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(ies) 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 October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

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 October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

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 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 October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.130.

(a) 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's 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 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(ies) 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(ies) 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's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.110, 1798.115, 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's 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); Stats. 2019, Ch. 757, Sec. 6.3 (AB 1355); and Stats. 2019, Ch. 759, Sec. 1.3 (AB 1564). Effective October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

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 webpage 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 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 webpage 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 $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% 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% 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, service mark 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 webpage, 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 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 webpage 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, family or 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. 748, Sec. 1.5 (AB 874) and Stats. 2019, Ch. 757, Sec. 7.5 (AB 1355). Effective October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.145.

(a) The obligations imposed on businesses by this title shall not restrict a business's 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 U.S. 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 U.S. 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 GLBA (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 CEO, 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% 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 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, nonprofit 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, nonprofit 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 CEO, 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% 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 January 1, 2021.

(Amended by Stats. 2019, Ch. 763, Sec. 2.3 (AB 25); Stats. 2019, Ch. 751, Sec. 2.3 (AB 1146); and Stats 2019, Ch. 757, Sec. 8.3 (AB 1355). Effective October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

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 $100 and not greater than $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 October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

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 $2,500 for each violation or $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 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, accessible to consumers with disabilities and 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 in to 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 October 11, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

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 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, 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.)

originally published 01/02/19

revised 01/24/20

Appendix B

CCPA: What To Disclose and Where To Disclose It

			WHO MUST DISCLOSE		WHERE TO DISCLOSE	
			Collector of personal information	Seller of personal information	Online privacy notice or website's "California Rights" section	Response to consumer access request
WHAT MUST BE DISCLOSED	Notice about PI processing	Categories of personal information collected about the consumer	X	X	X	X
		Categories of the sources from which the personal information was collected	X	X	X	X
		Business or commercial purpose for collecting or selling personal information	X	X	X	X
		Categories of third parties with whom the business shares personal information	X	X	X	X
		Specific pieces of personal information	X	X	X*	X
		Categories of personal information sold		X		X
		Categories of third parties to whom personal information was sold, by category or categories of personal information sold for each third party to whom personal information was sold		X		X
		Categories of personal information disclosed for a business purpose		X		X
		A list of the categories of personal information sold about consumers in the preceding 12 months or, if no sale occurred, that fact		X	X	X
		A list of categories of personal information disclosed for a business purpose in the preceding 12 months or, if no disclosure occurred, that fact		X	X	X

			WHO MUST DISCLOSE		WHERE TO DISCLOSE	
			Collector of personal information	Seller of personal information	Online privacy notice or website's "California Rights" section	Response to consumer access request
WHAT MUST BE DISCLOSED	Consumers' rights	To request access to their personal information, along with one or more designated methods for submitting such requests	X	X	X	
		To request deletion of their personal information	X	X	X	
		To opt out of the sale of their business information		X	X	
		Not to be discriminated against for exercising any of their other CaCPA rights	X	X	X	
	Financial incentives programs	Notice of any financial incentives pursuant to Section 1798.125(b)	X	X	X	
		Clear description of material terms of any financial incentive program	X	X	X	

*See discussion of: Section 1798.110(c)