

INITIAL STATEMENT OF REASONS (ISOR)

PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS (Stats. 2018, Ch. 55 [AB 375], as amended by Stats. 2018, Ch. 735 [SB 1121])

I. GENERAL PURPOSE OF PROPOSED REGULATIONS

The California Consumer Privacy Act (CCPA) was enacted in 2018 and will take effect on January 1, 2020. The CCPA confers new privacy rights for consumers and imposes corresponding obligations on businesses subject to it. The rights conferred to consumers include the right to know what personal information businesses are collecting about consumers and how that information is being used and shared, the right to delete personal information held by businesses, the right to stop the sale of personal information by businesses, and the right to non-discrimination in service and price when exercising privacy rights. (Civ. Code, §§ 1798.100-1798.199.)

These regulations are intended to operationalize the CCPA and provide clarity and specificity to assist in the implementation of the law. The CCPA requires the Attorney General to adopt initial regulations on or before July 1, 2020. (Civ. Code, § 1798.185, subd. (a).) The Office of the Attorney General submits these proposed regulations to fulfill this mandate, and to provide guidance to consumers and businesses subject to the CCPA. The purpose of each specific provision of these proposed regulations is set forth in Section IV below.

II. PROBLEM INTENDED TO ADDRESS

The California Legislature stated the need for enhanced consumer privacy rights in its findings for AB 375, noting that although California has been a leader in privacy protection, the law has not kept pace with rapid technological developments and the proliferation of personal information that fuels the internet economy. As a result, consumers are largely unable to control or even understand the collection and use of their personal information by a myriad of businesses and organizations.

The Legislature further describes some of the consequences of the lack of adequate privacy laws: “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.”

The CCPA addresses this problem by providing consumers with new privacy rights and imposing corresponding obligations on businesses. It vests consumers with the right to know details about how their personal information is collected, used, and shared by businesses; the right to take control of their information by having businesses delete it and stop selling it; and the right to exercise these privacy rights without suffering discrimination in price or service. It also requires businesses to provide consumers with notices of their rights under CCPA and to respond to consumer requests to exercise such rights.

The proposed regulations are authorized and largely mandated by the CCPA. The CCPA requires the Attorney General to adopt regulations to guide businesses in fulfilling their obligations under the CCPA. The CCPA specifies certain areas for the regulations, outlined in Section I above. In some cases, it conditions businesses' ability to comply with the CCPA on the Attorney General's regulations. It also authorizes the Attorney General to adopt additional regulations as necessary to further the purposes of the CCPA.

Section IV below details the specific purpose and rationale for why the regulations are reasonably necessary to carry out the purpose of the CCPA, as well as the benefits anticipated from the regulatory action. It also identifies the technical, theoretical, or empirical studies, reports, or similar documents relied upon in proposing the regulations, any reasonable alternatives considered, and to the extent that the regulation mandates a specific action or procedure, why the Attorney General believes these mandates are required.

III. SUMMARY OF BENEFITS

The regulations will benefit the welfare of California residents because they will facilitate the implementation of many components of the CCPA. By providing clear direction to businesses on how to inform consumers of their rights and how to handle their requests, the regulations will make it easier for consumers to exercise their rights. The regulations on notice, for example, will promote greater transparency to the public regarding how businesses collect, use, and share personal information and on what businesses must do to comply with the CCPA. The regulations on timing and record-keeping will encourage businesses to provide complete and timely responses to consumer requests.

The increased individual control over personal information granted by the law and specified in the regulations can also protect consumers from some abuses of that information, such as discrimination, harassment, and fraud. In the very tangible case of identity theft, a recent study found that the total out-of-pocket cost to victims in 2018 was \$1.7 billion. (Javelin Strategy & Research (March 2019) *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt*, p. 10, Figure 1.)

Privacy is one of the inalienable rights conferred on Californians by the state Constitution. The CCPA enumerates specific privacy rights. In giving consumers greater control over their personal information, the CCPA, operationalized by these regulations, mitigates the asymmetry of knowledge and power between individuals and businesses. This benefits not only individuals, but society as a whole. The empowerment of individuals to exercise their rights is particularly important for a democracy, which values and depends on the autonomy of the individuals who constitute it.

IV. PROPOSED REGULATIONS – PURPOSE, NECESSITY, AND BENEFITS

A. 11 CCR § 999.300. Title and Scope

Subdivision (a) provides that Chapter 20 shall be known as the “California Consumer Privacy Act Regulations” and will be referred throughout the Chapter as “these regulations.” It also states

that the regulations govern compliance with the CCPA and do not limit any other rights that consumers may have. The purpose of this regulation is to establish the scope of the new chapter. It is necessary to identify the title for reference throughout the regulations and to explain the scope of the regulations.

Subdivision (b) provides that a violation of these regulations shall constitute a violation of the CCPA, and be subject to the remedies provided for therein. The purpose of this regulation is to identify the relationship between the CCPA and the regulations. It is necessary to clarify that the regulations are an extension of the CCPA, and thus, subject to the enforcement scheme and remedies provided for in the CCPA.

B. 11 CCR § 999.301. Definitions

Subdivisions (a) through (u) of this section define terms used throughout this Chapter. It is necessary to define these terms because many of them could have multiple meanings depending on the context of their usage. Furthermore, some of the terms are used in the CCPA without being defined. Defining the terms clarifies the meaning of the regulations and helps eliminate any misunderstandings or confusion between the Attorney General and the public. It assists businesses in implementing the law, as well as the regulations, and thereby increases the likelihood that consumers will enjoy the benefits of the rights provided them by the CCPA.

Subdivision (a) establishes that “affirmative authorization” means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13 years of age, it means that the parent or guardian has provided consent to the sale of the child’s personal information in accordance with the methods set forth in section 999.330 of these regulations. For consumers 13 years of age and older, it is demonstrated through a two-step process whereby the consumer first, clearly requests to opt-in and then second, separately confirms the choice to opt-in. The purpose of defining this term is to provide clarity on the procedures regarding the sale of the personal information of minors set forth in these regulations and to avoid any confusion that may result from different understandings of the term. This definition is necessary because Civil Code section 1798.120, subdivision (c), uses the term without defining it, and the procedure it represents is essential to ensure the proper handling of children’s personal information.

Subdivision (b) establishes that “Attorney General” means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General. The purpose of defining this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the term. This definition is necessary because the CCPA does not define it and the law and these regulations may be enforceable against businesses located in other states that have their own attorneys general.

Subdivision (c) establishes that an “authorized agent” means a natural person or a business entity registered with the Secretary of State that a consumer has authorized to act on the consumer’s behalf subject to the requirements set forth in section 999.326 of these regulations. The purpose of defining this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the term. The definition is necessary because the term is not defined in the CCPA although it is used several times. The definition is based on language used in Civil Code section 1798.140, subdivision (y), wherein the definition of a

“verifiable consumer request” includes one made by “a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf.”

Subdivision (d) establishes that “categories of sources” means the types of entities from which a business receives personal information about consumers, including but not limited to, the consumer directly, government entities from which public records are obtained, and consumer data resellers. The purpose of defining this term is to provide clarity and guidance regarding one of the disclosures required by the CCPA and specified in these regulations. Civil Code sections 1798.110 and 1798.130 require businesses to disclose the “categories of sources” from which they collect personal information about consumers, but does not otherwise define the term. This definition identifies key sources of personal information for a business, while at the same time leaving the list open-ended to allow for differing business practices. This benefits consumers by ensuring enough specificity for consumers to understand the businesses’ data practices. It also benefits businesses, particularly smaller businesses that lack privacy resources, by clarifying the categories they must identify.

Subdivision (e) establishes that “categories of third parties” means “types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.”

The purpose of defining this term is to provide clarity and guidance on one of the disclosures required by the CCPA and specified in these regulations. The CCPA requires businesses to disclose the categories of third parties with whom they share personal information (Civ. Code, §§ 1798.110, subd. (a) & (c), 1798.130, subd. (a)(5)), but while it defines “third parties,” it does not define “categories of third parties.”

This definition identifies key categories of third parties, while at the same time leaving the list open-ended to allow for differing business practices. The categories are drawn primarily from the work of a year-long multi-stakeholder process facilitated by the National Telecommunications and Information Administration in the U.S. Department of Commerce, in 2013. The process, which involved the participation of representatives of numerous businesses, industry organizations, and consumer and privacy advocates, resulted in a voluntary code of conduct for a privacy notice that would give consumers enhanced transparency about the data collection and sharing practices of mobile applications. The list of categories of third-party entities is part of the code of conduct and is relevant not just for the mobile ecosystem but for the broader spectrum of businesses that collect personal information. (National Telecommunications and Information Administration, U.S. Department of Commerce, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* (July 25, 2013) p. 3.)

The definition benefits consumers by ensuring enough specificity for consumers to understand the businesses’ data practices. It also benefits businesses, particularly smaller businesses that lack privacy resources, by clarifying the categories they must identify.

Subdivision (f) establishes that “CCPA” means the California Consumer Privacy Act of 2018, Civil Code section 1798.100 *et seq.* The purpose of defining this term is to make the regulations more readable, and thus, easier for consumers and businesses to understand. This definition is necessary because without it, the lengthy full title of the act would occur repeatedly throughout the regulations.

Subdivision (g) establishes that “financial incentive” means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information. Civil Code section 1798.185, subdivision (a)(6), directs the Attorney General to establish rules and guidelines regarding financial incentive offerings, but does not define the term. The purpose of defining this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the term.

Subdivision (h) establishes that “household” means a person or group of people occupying a single dwelling. The term “household” appears in the definitions of a number of important terms in the CCPA (*i.e.*, “personal information,” “business,” and “health insurance information”), but is not otherwise defined. The purpose of defining this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the word. The definition is based on standard dictionary definitions of the word.

Subdivision (i) establishes that “notice at collection” means “the notice given by a business to a consumer at or before the time a business collects personal information from the consumer as required by Civil Code section 1798.100(b) and specified in these regulations.”

The purpose of defining this term is to provide clarity and guidance on one of the disclosures required by the CCPA and specified in these regulations. The definition is intended to help businesses implement the regulations by giving a name to the notice required by Civil Code section 1798.100, subdivision (b), regarding the notice required at or before the collection of personal information. This definition clearly distinguishes the notice at collection from other notices required by the CCPA, and assists businesses with making the notice easily understandable and accessible to consumers, as required by Civil Code section 1798.185, subdivision (a)(6). It also makes these regulations more readable, and thus, easier for consumers and businesses to understand.

Subdivision (j) establishes that “notice of right to opt-out” means “the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.”

The purpose of defining this term is to provide clarity and guidance on one of the disclosures required by the CCPA and specified in these regulations. The definition is intended to help businesses implement the regulations by giving a name to the notice required by Civil Code section 1798.120, regarding the right to opt-out of the sale of personal information. This definition clearly distinguishes the notice of right to opt-out from other notices required by the CCPA and assists businesses with making the notice easily understandable and accessible to consumers, as required by Civil Code section 1798.185, subdivision (a)(6). It also makes these regulations more readable, and thus, easier for consumers and businesses to understand.

Subdivision (k) establishes that “notice of financial incentive” means “the notice given by a business explaining each financial incentive or price or service difference subject to Civil Code section 1798.125(b) as required by that section and specified in these regulations.”

The purpose of defining this term is to provide clarity and guidance on one of the disclosures required by the CCPA and specified in these regulations. The definition is intended to help businesses implement the regulations by giving a name to the notice required by Civil Code section 1798.125, subdivision (b)(2), regarding the prohibition on discrimination based on a

consumer's exercise of rights under the CCPA. Businesses are required to notify consumers of any financial incentives offered in compensation for the collection, sale, or deletion of personal information. This definition clearly distinguishes the notice of financial incentive from other notices required by the CCPA and assists businesses with making the notice easily understandable and accessible to consumers, as required by Civil Code section 1798.185, subdivision (a)(6). It also makes these regulations more readable, and thus, easier for consumers and businesses to understand.

Subdivision (l) establishes that “price or service difference” means any difference in the price or rate charged for any goods or services to any consumer, including through the use of discounts, financial payments, or other benefits or penalties; or any difference in the level or quality of any goods or services offered to any consumer, including denial of goods or services to the consumer. The purpose of this term is to provide clarity to the regulations and to make the regulations more readable. This definition is necessary because the concept is central to the CCPA's provisions on non-discrimination in Civil Code section 1798.125, but not otherwise defined. The definition here summarizes the concept described in section 1798.125 and allows a shortened phrase to be used throughout the regulations, making them more readable, and thus, easier for consumers and businesses to understand.

Subdivision (m) establishes that “privacy policy” means “the policy referred to in Civil Code section 1798.130(a)(5), and means the statement that a business shall make available to consumers describing the business's practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their own personal information.”

The purpose of defining this term is to provide clarity and guidance on one of the disclosures required by the CCPA and specified in these regulations. The definition is intended to help businesses implement the regulations by giving a name to the notice required by Civil Code section 1798.130, subdivision (a)(5), regarding a business's public-facing privacy policy. The CCPA requires businesses to post a privacy policy on their website containing specified information about their privacy practices and to update the policy at least once every 12 months. It does not delineate between a business's online or offline practices. Thus, this definition clarifies that while Civil Code section 1798.130 refers to an “online privacy policy,” the policy is to cover both offline and online practices. The definition further assists businesses with making the notice easily understandable and accessible to consumers, as required by Civil Code section 1798.185, subdivision (a)(6). It also makes these regulations more readable, and thus, easier for consumers and businesses to understand.

Subdivision (n) establishes that “request to know” means a consumer request that a business disclose personal information that it has about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following: (1) specific pieces of personal information that a business has about the consumer; (2) categories of personal information it has collected about the consumer; (3) categories of sources from which the personal information is collected; (4) categories of personal information that the business sold or disclosed for a business purpose about the consumer; (5) categories of third parties to whom the personal information was sold or disclosed for a business purpose; and (6) the business or commercial purpose for collecting or selling personal information.

The purpose of defining the term is to provide clarity to the regulations and to make them more readable. The definition is necessary to clearly identify and avoid any confusion regarding which requests the regulations are referring to when setting forth the rules and procedures businesses must follow. It allows the regulations to group together the requirements businesses must follow in responding to certain consumer requests. It also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subdivision (o) establishes that “request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105. The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase “request to delete” also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subdivision (p) establishes that “request to opt-out” means a consumer request that a business not sell the consumer’s personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a). The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase “request to opt-out” also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subdivision (q) establishes that “request to opt-in” means the affirmative authorization that the business may sell personal information about the consumer required by Civil Code section 1798.120, subdivision (c), by a parent or guardian of a consumer less than 13 years of age, or by a consumer who had previously opted out of the sale of their personal information. The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase “request to opt-in” also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subdivision (r) establishes that “third-party identity verification service” means a security process offered by an independent third party who verifies the identity of the consumer making a request to the business. Third-party verification services are subject to the requirements set forth in Article 4 of these regulations regarding requests to know and requests to delete. The purpose of defining this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the term. This definition is necessary because Civil Code 1798.185 directs the Attorney General to establish rules and procedures for governing a business’s determination that a request received from a consumer is a “verifiable request.” Many businesses currently use third-party verification systems to verify consumer identities, and thus, it is included in section 999.323, subdivision (b)(1) as a means to verify a consumer’s request.

Subdivision (s) establishes that “typical consumer” means a natural person residing in the United States. The purpose of this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the term. This definition is necessary for the regulations on non-discrimination in Article 6, in particular for provisions on how businesses are to calculate the value of consumer data when offering financial incentives, section 999.337, subdivision (b), of these regulations.

Subdivision (t) establishes that “URL” stands for Uniform Resource Locator and refers to the web address of a specific website. The purpose of this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the term. This

definition is necessary for the regulations on the notice of right to opt-out in section 999.306 of these regulations, which implements Civil Code sections 1798.135 on the placement of the notice. The definition is based on the standard dictionary definition of the term.

Subdivision (u) establishes that “verify” means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information. The purpose of defining this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the term. This definition is necessary for Article 4 on verification of consumer requests, implementing Civil Code, section 1798.185, subdivision (a)(7), which directs the Attorney General to establish rules and procedures for, among other things, how a business should determine that a request received from a consumer constitutes a verifiable request. The definition also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

C. 11 CCR § 999.305. Notice at Collection of Personal Information

Civil Code section 1798.100, subdivision (b), requires a business that collects a consumer’s personal information to inform consumers, at or before the point of collection, of the categories of personal information it collects and the purposes for which the categories are used. The purpose of section 999.305 of these regulations is to set forth the rules and procedures businesses must follow regarding the form, content, and posting of the notice at collection. Bringing together the requirements distributed among different sections of the CCPA, the regulation is necessary to ensure that the notice contains the information required in Civil Code section 100, subdivision (b), and is provided in a manner that makes it easily accessible and understandable to consumers, including those with disabilities, as required by Civil Code section 1798.185, subdivision (a)(6).

Subdivision (a)(1) and (2) clarify the purpose for the notice at collection and provide general principles for making the notice accessible and comprehensible. These subdivisions are necessary because studies have found that presentation and the use of plain language techniques positively influence the effectiveness and comprehension of privacy policies. (See Schaub, et al., *A Design Space for Effective Privacy Notices* (July 22–24, 2015) Symposium on Usable Privacy and Security (SOUPS) 2015, Ottawa, Canada (hereafter Schaub); Center for Plain Language, *Privacy-policy analysis* (2015) (hereafter Center for Plain Language).) The subdivisions recognize that the notice at collection will be provided in a variety of contexts, both online and offline, because of the wide range of businesses subject to the CCPA. Thus, the subdivisions take a performance-based approach, calling for the notices to be designed and presented in a way that makes them easy to read and understandable by consumers, with some specific requirements drawn from the studies to further those ends.

Subdivision (a)(3) and (4) restricts businesses from collecting or using personal information beyond what was disclosed in the notice at collection. Subdivision (a)(3) requires a business that intends to use a consumer’s personal information for a purpose not disclosed in the notice at collection to directly notify the consumer and obtain explicit consent for the new use. Subdivision (a)(4) requires a business that intends to collect new categories of personal information not disclosed in the notice at collection to provide a separate, updated notice at collection. The purpose of these subdivisions is to implement Civil Code section 1798.100, subdivision (b). The subdivisions make clear that a business cannot change their practices after

giving the notice at collection because the consumer could have reasonably relied on the information provided in the notice at collection when interacting with the business.

Subdivision (a)(5) prohibits the collection of personal information from the consumer if a business does not give the notice at collection to the consumer at or before the collection of their personal information. The purpose of this subdivision is to implement Civil Code section 1798.100, subdivision (b). The subdivision makes clear that businesses that collect personal information without first giving notice to the consumer are in violation of Civil Code section 1798.100 and these corresponding regulations. It clearly prohibits the surreptitious collection of personal information.

Subdivision (b) describes the contents of the notice at collection, implementing Civil Code section 1798.100, subdivision (b). The subdivision requires the notice to include a list of the categories of personal information to be collected and, for each category, the purpose for which the personal information will be used. In addition, the subdivision requires a business that sells personal information to include the “Do Not Sell My Personal Information” link required by section 999.315, subdivision (a), of these regulations, or in the case of an offline notice, the web address for the webpage to which it links.

This subdivision furthers the purposes of the notification requirement by allowing consumers to opt-out at the earliest point in time that the information is collected. This prevents any delay that may lead to the dissemination of the consumer’s information against the consumer’s wishes. The subdivision also requires that the notice include a link to the business’s privacy policy, which allows the consumer easy access to a comprehensive explanation of the business’s privacy practices.

Subdivision (c) provides a compliance option for businesses that collect personal information online, allowing them to provide the notice at collection by linking to the section of their privacy policy that contains the required information for the notice, rather than to a separate notice webpage. Such an approach can result in some reduction of the work involved in updating consumer privacy notices. The subdivision gives businesses greater flexibility, simplifying the process of keeping notices updated without lessening consumer benefits.

Subdivision (d) addresses businesses, such as data brokers, that do not collect personal information directly from consumers, and thus, are not in a position to provide a notice at collection to consumers at or before the time of collection. The subdivision provides that those businesses do not have to provide a notice at collection, but they must ensure that consumers were given explicit notice of the sale of their personal information and an opportunity to opt-out. The business can do so by either: (1) contacting the consumers directly to give the required notice and opportunity to opt-out; or (2) contacting the sources of the personal information to confirm that they provided the notice at collection to the consumer. If the business contacts the source, it must obtain a signed attestation from the source describing how the notice at collection was given and attaching an example of the notice. Businesses must retain copies of the attestations for at least two years and make them available to the consumer upon request. Since such businesses collect personal information primarily in order to sell it, the subdivision will provide consumers with more effective notification of the business’s collection practices than any alternative.

The purpose of this subdivision is to implement Civil Code section 1798.115, subdivision (d), which prohibits third-party businesses from selling consumers' personal information unless the consumers are given explicit notice and an opportunity to opt-out of the sale of their information. It instructs businesses that do not have direct contact with consumers on how to comply with Civil Code section 1798.115, subdivision (d), and furthers the purposes of the CCPA by ensuring that consumers have an opportunity to opt-out of the sale of their personal information before it is sold by those businesses. This subdivision is necessary because it addresses questions and comments raised by interested parties during the Attorney General's preliminary fact-gathering rulemaking activities.

D. 11 CCR § 999.306. Notice of Right to Opt-Out of Sale of Personal Information

Civil Code section 1798.120, subdivision (b), requires all businesses covered by the CCPA that sell personal information to provide notice to consumers of their right to opt-out of such sale pursuant to Civil Code section 1798.135. The purpose of section 999.306 of these regulations is to set forth the rules and procedures businesses must follow regarding the form, content, and posting of the notice of right to opt-out. The regulation also addresses situations where a business may not maintain a website or primarily interacts with consumers offline. The regulation is necessary in order to ensure that the notice of right to opt-out contains the information required in Civil Code section 1798.135, subdivision (a), and is provided in a manner that makes it easily accessible and understandable to consumers, including those with disabilities, as required by Civil Code section 1798.185, subdivision (a)(6).

Subdivision (a) clarifies the purpose for the notice of right to opt-out and provides general principles for making the notice accessible and comprehensible. The subdivision is necessary because studies have found that presentation and the use of plain language techniques positively influence the effectiveness and comprehension of privacy policies. (See Schaub; Center for Plain Language.) The subdivision takes a performance-based approach, calling for the notice to be designed and presented in a way that makes it easy to read and understandable by consumers.

Subdivision (b) implements Civil Code section 1798.135, subdivision (a), regarding how to make the notice of right to opt-out reasonably accessible to consumers. It recognizes that there are businesses, primarily smaller ones, that may not have websites and whose interactions occur generally offline, and guides them on how they can provide the notice of right to opt-out. The subdivision addresses conspicuous website postings, and takes a performance-based approach for businesses that do not have a website, requiring them to establish another method for informing consumers of the right to opt-out. The subdivision also takes a performance-based approach for businesses whose interactions with consumers are substantially offline, requiring them to use an offline method that facilitates consumer awareness and offering a non-exclusive list of examples of such methods. The subdivision also provides compliance options for businesses by allowing them to provide the notice of right to opt-out by linking to a portion of its privacy policy that contains the information required in section 999.306, subdivision (d), rather than linking to a separate opt-out notice webpage.

Subdivision (c) specifies the contents of the notice of right to opt-out, implementing Civil Code section 1798.135, subdivision (a)(2) and subdivision (c). This subdivision clarifies what must be included in the notice of right to opt-out and explains that the notice is to be posted on the "Do

Not Sell My Personal Information” webpage, along with a webform by which a consumer can submit their request to opt-out online. In the case of a business without a website, the business must include the offline method for submitting such a request. In addition, the subdivision requires the notice to include other information helpful to a consumer considering their right to opt-out, such as information about the use of an authorized agent to submit the request on the consumer’s behalf and a link to the business’s privacy policy. The subdivision is necessary because requirements regarding the right to opt-out are set forth in different parts of the CCPA and need to be harmonized (Civ. Code, §§ 1798.120, 1798.135, and 1798.185). For example, it clarifies the relationship between the notice of the right to opt-out required by Civil Code section 1798.120, subdivision (b), and the “Do Not Sell My Personal Information” link, required by Civil Code section 1798.135, subdivision (a)(1), and section 999.315 of these regulations.

Subdivision (d) implements Civil Code section 1798.185, subdivision (a)(4) and (a)(6), clarifying the exceptions to the requirement for businesses to provide consumers with the notice of right to opt-out. The subdivision requires a business that is exempt from notification on the basis that it does not sell personal information to explicitly state so in its privacy policy. This requirement is necessary to provide transparency for consumers, both by providing information in the privacy policy and by avoiding the potentially confusing posting of a notice of right to opt-out by a business that does not sell personal information. It also promotes data governance and accountability by requiring a business to ensure that it complies with its posted policy.

The subdivision also addresses a situation where a business that is exempt from posting an opt-out notice later decides to sell personal information, including information it had collected during the period it did not post a notice of right to opt-out. Because selling a consumer’s personal information without giving them notice and the opportunity to opt-out goes against the intent and purposes of the CCPA, the subdivision requires the business to treat personal information collected from the consumer during the time it did not post a notice of right to opt-out as if the consumer had submitted a request to opt-out.

Subdivision (e) implements Civil Code section 1798.185, subdivision (a)(4), regarding the development and use of a uniform opt-out button or logo to promote consumer awareness of the opt-out right. The subdivision provides that the button or logo, which will be added in a modified version of the regulations and made available for public comment after the 45-day public comment period, may be used in addition to, but not in lieu of, the posting of the notice of right to opt-out. The button or logo is to link to the webpage or online location containing the information specified in section 999.306, subsection (c). The subdivision notes that the button or logo will be added in a modified version of the regulations at a later date because the Attorney General wishes to consider public feedback on its design. Public engagement in the development of the button or logo is necessary to increase the likelihood that users will recognize and use the button or logo.

E. 11 CCR § 999.307. Notice of Financial Incentive

Civil Code section 1798.125, subdivision (b), requires businesses that offer any financial incentives to notify consumers of the financial incentives pursuant to Civil Code section 1798.130. The purpose of section 999.307 of these regulations is to set forth the rules and procedures businesses must follow regarding the form, content, and posting of the notice of financial incentive. The regulation is necessary to ensure that the notice contains the information

necessary for a consumer to consent to participate, as required by Civil Code section 1798.125, subdivision (b)(3), and is provided in a manner that makes it easily accessible and understandable to consumers, including those with disabilities, as required by Civil Code section 1798.185, subdivision (a)(6).

Subdivision (a) clarifies the purpose for the notice of financial incentive and provides general principles for making the notice accessible and comprehensible. The subdivision is necessary because studies have found that presentation and the use of plain language techniques positively influence the effectiveness and comprehension of privacy policies. (See Schaub; Center for Plain Language.) The subdivision takes a performance-based approach, calling for the notices to be designed and presented in a way that makes them easy to read and understandable by consumers. It also provides compliance options for businesses by allowing them to provide the notice by linking to a portion of its privacy policy that contains the information required in section 999.307, subdivision (b), rather than linking to a separate or standalone webpage.

Subdivision (b) specifies the content of the notice of financial incentive, implementing Civil Code sections 1798.125, subdivision (b)(3), and 1798.130. The subdivision requires the notice to provide sufficient information to enable a consumer to make an informed decision, including both the consumer benefits and costs. The notice must include not just a description of the material terms of the incentive (pursuant to Civil Code section 1798.125, subdivision (b)(3)), but the categories of personal information implicated by the consumer's participation in the financial incentive. The notice must also describe how the consumer can opt-in or consent to the incentive and how the consumer may withdraw consent. Requiring information on how to consent and how to withdraw consent is consistent with basic fairness in consumer transactions, including those that involve a consumer's data.

The notice must also explain why the financial incentive is permitted under the CCPA. The explanation must include an estimate of the value of the consumer's data and a description of how the business determined the value. Civil Code section 1798.125 prohibits a business from discriminating against a consumer for exercising their rights under the CCPA, but allows the offering of financial incentives if they are directly related to the value of the consumer's personal information. In order to assist the consumer in evaluating the trade-off provided by a financial incentive, subdivision (b) requires the notice of financial incentive to provide an explanation of why the incentive is permitted under the CCPA. This explanation must include both a description of the business's good-faith estimate of the value of the data that forms the basis for offering the incentive and a description of the method the business used to calculate the value of the data. (See discussion of §§ 999.336 and 999.337 below.)

The elements required by the subdivision are essential to further the CCPA's purpose of prohibiting discrimination based on a consumer's exercise of privacy rights. Without knowing the categories of personal information involved and how the business values them, a consumer would not be in a position to make informed decisions on whether to opt-in to the offered financial incentives. Requiring this information gives consumers a full picture of the costs and benefits of the incentive and provides greater transparency to consumers about the business's practices. It also increases businesses' accountability to the law by disclosing information necessary for the public and the Attorney General to evaluate whether the financial incentive is in fact reasonably related to the value of the data.

F. 11 CCR § 999.308. Privacy Policy

Civil Code section 1798.130, subdivision (a)(5), requires a business to disclose certain information in its privacy policy and to update that information at least once every 12 months. The purpose of section 999.308 of these regulations is to set forth the rules and procedures businesses must follow regarding the form, content, and posting of the privacy policy. The regulation is necessary to ensure that the privacy policy contains the necessary information and is provided in a manner that makes it easily accessible and understandable to consumers, including those with disabilities, as required by Civil Code section 1798.185, subdivision (a)(6).

Subdivision (a)(1) clarifies the purpose of the privacy policy, which is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of consumer personal information and of the rights of consumers regarding their personal information. The privacy policy provides in one place all the disclosures required by the CCPA, including explanations of the consumer privacy rights conferred by it. Although Civil Code section 1798.130, subdivision (a)(5), refers to an "online privacy policy," the stated intent of the California Legislature in enacting the CCPA was to provide consumers with rights to control their personal information. The CCPA did not limit those rights to only personal information a business collects online. Accordingly, this subdivision clarifies that the privacy policy must cover the business's privacy practices both online and offline. The use of the term "online privacy policy" refers to the usual location of a privacy policy on a business's website, not to any limitation on the scope of the privacy policy.

Subdivision (a)(1) also clarifies that a business's privacy policy does not need to be personalized for each consumer and should not contain specific pieces of consumers' personal information. This is in response to public comments submitted to the Attorney General in the preliminary rulemaking process expressing concern that Civil Code section 1798.110, subdivision (c), could be interpreted to mean that specific pieces of personal information are to be included in a business's privacy policy, rather than in response to a consumer's request.

Subdivision (a)(2) provides general principles for making the privacy policy accessible and comprehensible. The subdivision is necessary because studies have found that presentation and the use of plain language techniques positively influence the effectiveness and comprehension of privacy policies. (See Schaub; Center for Plain Language.) The subdivision takes a performance-based approach, calling for the notice to be designed and presented in a way that is easy to read and understandable by consumers. The subdivision implements Civil Code section 1798.130, subdivision (a)(5), requiring a business to post the privacy policy online through a conspicuous link using the word "privacy" on the business's website homepage and, if the business has a California-specific description of privacy rights on its website, then posting the privacy policy must be included there.

Subdivision (a)(3) implements and clarifies Civil Code section 1798.130, subdivision (a)(5), instructing businesses where and how to post their privacy policies. This subdivision is necessary to inform both online and offline businesses about how to comply with the privacy policy provisions in the CCPA. It specifies that if a business has a California-specific description of consumers' privacy rights on its website, the policy should be included there, and that in any case the privacy policy must be made available through a conspicuous link on the business's homepage or the download or landing page of a mobile app. The subdivision also provides that

the policy may be included in a California-specific description of consumers' privacy rights. It also provides that businesses without a website must make the privacy policy conspicuously available to consumers by some other means. It is important to assist such businesses, which are likely to be smaller businesses, by authorizing the use of offline means to achieve the intended objective of making their privacy policy available to consumers.

Subdivision (b) specifies the contents of the privacy policy, implementing Civil Code section 1798.130, subdivision (a)(5), and the other referenced sections concerning notices to consumers referenced therein (Civ. Code, §§ 1798.110, 1798.115, and 1798.125). The subdivision provides that the privacy policy must explain the CCPA's consumer privacy rights and the procedures for consumers to make requests under those rights, as well as a description of the business's practices regarding the personal information it collects or maintains on consumers. This subdivision presents the contents of the privacy policy under each of the CCPA's consumer privacy rights. This organization is intended to clarify the requirements but not to prescribe the organization of any business's privacy policy.

In addition to the contents specifically required in Civil Code section 1798.130, subdivision (a)(5), the subdivision also requires the privacy policy to include other information helpful to consumers, including an explanation of the procedure for a consumer to designate an authorized agent to act on the consumer's behalf in submitting requests to businesses, as provided in Civil Code section 1798.185, subdivision (a)(7), and a designated contact to answer consumers' questions on the business's privacy policies and practices. The subdivision also provides that the privacy policy must contain the date it was last updated to ensure the public that it has been updated within the preceding 12 months, as required by Civil Code section 1798.130, subdivision (a)(5).

For businesses that buy, receive, sell, or share for commercial purposes the personal information of more than four million consumers, which is roughly 10 percent of the state's population, the subdivision requires the disclosure of certain metrics within their privacy policy, as specified in section 999.317, subdivision (g), of these regulations. The purpose of requiring this information in the privacy policy is to provide transparency to the public about the exercise of consumer privacy rights under the CCPA. This information will also help policymakers, academics, regulators, and consumers evaluate the effectiveness of business practices and compliance with the CCPA.

The subdivision is necessary because it provides a comprehensive picture of a business's privacy practices and of how consumers can exercise their rights under the CCPA. The subdivision pulls together in one place the statutory requirements for the policy, which are distributed throughout the CCPA, and other helpful information, making the privacy policy a useful resource for consumers and others interested in evaluating the effectiveness of the CCPA.

G. 11 CCR § 999.312. Methods for Submitting Requests to Know and Requests to Delete

Civil Code sections 1798.100, 1798.110, and 1798.115 provides consumers with the right to request a business to disclose personal information that it has about the consumer (*i.e.*, request to know), and Civil Code section 1798.105 provides consumers with the right to request the deletion of personal information a business has collected from the consumer about them (*i.e.*, request to delete). The purpose of section 999.312 of these regulations is to set forth the rules and

procedures businesses must follow regarding how consumers are to submit these requests to know and requests to delete. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(7), requires the Attorney General to establish rules and procedures to further the purposes of sections 1798.110 and 1798.115, and to facilitate the ability of a consumer or a consumer's authorized agent to obtain information pursuant to section 1798.130, which addresses sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125. Section 1798.140, subdivision (i), also requires the Attorney General to approve "designated methods for submitting requests" under the CCPA. Section 1798.185(a)(7) further provides that the regulations should have the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business.

Subdivision (a) requires a business to provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business maintains a website, a link or form available online through the business's website. It also specifies that other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail. This subdivision is necessary to provide clarity for businesses receiving consumer requests under the CCPA. Although a consumer's right to request that a business disclose personal information is set forth in Civil Code sections 1798.100, 1798.110, and 1798.115, section 1798.130, subdivision (a)(1), only identifies sections 1798.110 and 1798.115 when requiring two methods for submitting requests. This subdivision requires businesses to have the same procedure for requests to know made pursuant to section 1798.100 as for requests to know made pursuant to sections 1798.110 and 1798.115. This benefits both the business and consumers by simplifying the procedure, which will in turn allow more consumers to exercise their right to know. This subdivision also identifies other acceptable methods that the business can adopt as ways for a consumer to submit their requests to know, giving businesses clarity on how to comply with the law.

Subdivision (b) requires a business to provide two or more designated methods for submitting requests to delete. It specifies that acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail. This subdivision is necessary because the CCPA is silent regarding the procedures by which consumers are to submit requests to delete and businesses are to respond to those requests. This subdivision aligns the process for requests to delete with those for requests to know, which reduces the potential for confusion on the part of consumers and businesses. It does not prescribe, however, a particular method for submission of requests to delete because that is not required by the CCPA. This approach provides businesses greater flexibility to adopt methods that are most compatible with their business practices.

Subdivision (c) requires a business to consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. It requires that at least one method offered reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods for submitting requests to know. It also provides two illustrative examples of how to comply with this requirement. This subdivision is necessary because it prevents businesses from picking obscure methods for submitting requests as a way of discouraging consumers from exercising their rights.

Subdivision (d) requires a business to use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted. This subdivision is necessary because it provides consumers the opportunity to correct an accidental decision that may lead to the irrevocable deletion of personal information. It also provides businesses additional assurance that the consumer has made a clear choice to exercise their right to delete.

Subdivision (e) requires a business that does not interact directly with consumers in its ordinary course of business, such as data brokers, to offer at least one online method by which a consumer may submit requests to know or requests to delete. This subdivision is necessary because it prevents these businesses from only offering methods that would be difficult or onerous for the consumer to utilize. An online method for submitting requests is low in cost for both consumers and businesses, and conveniently accessible to consumers in different physical locations.

Subdivision (f) provides that if a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either: (1) treat the request as if it had been submitted in accordance with the business's designated manner, or (2) provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable. This subdivision is necessary to prevent a business from using technical or correctable deficiencies as an excuse to deny a request. It gives the consumer an opportunity to remedy any incorrect submission of a request and provides transparency to the whole process.

H. 11 CCR § 999.313. Responding to Requests to Know and Requests to Delete

The purpose of section 999.313 of these regulations is to set forth the rules and procedures businesses must follow in responding to consumer requests made pursuant to Civil Code sections 1798.100, 1798.105, 1798.110, and 1798.115 to the business. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(7), requires the Attorney General to establish rules and procedures to further the purposes of sections 1798.110 and 1798.115, and to facilitate a consumer's or a consumer's authorized agent's ability to obtain information pursuant to section 1798.130, which addresses sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125. Section 1798.185, subdivision (a)(7), further provides that the regulations should have the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business.

Subdivision (a) requires that upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 days and provide information about how the business will process the request, the business's verification process, and when the consumer should expect a response, except in instances where the business has already granted or denied the request. Setting a timeline for a business to provide initial confirmation of the request is necessary to help consumers understand the process and know when they should expect a complete response. The subdivision benefits businesses by helping manage consumer expectations. The subdivision's 10-day response time is also reasonable because it does not require that a business provide any immediate individualized information; rather the business is to confirm receipt and explain the process for handling the request to the consumer. This initial response can be prepared ahead of time and automated to lessen the cost to the business. The

caveat that the business need not provide this response if the business has already granted or denied the request takes into consideration those instances where a business may grant or deny the consumer's request before the 10 days, thus rendering this response unnecessary.

Subdivision (b) requires businesses to substantively respond to requests to know and requests to delete within 45 days. It specifies that the 45-day period will begin on the day that the business receives the request, regardless of the time required to verify the request. It also allows a business to take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the business receives the request, if the business provides the consumer with notice and an explanation of the reason why it will take longer. Consumers exercising their rights to make requests under the CCPA should not be hindered by unreasonable delays, and 45 to 90 days provide businesses with sufficient time to provide the required response. This timeframe is longer than historical response times for notifying consumers of a data breach. As noted in the California Attorney General's 2016 report on four years of data breaches, the average time of consumer notification was 40 days, with a median time of 30 days. (California Department of Justice, Attorney General's Office, *California Data Breach Report* (February 2016), p. 25.)

This subdivision is necessary because the CCPA has two conflicting provisions regarding the timing to respond to requests. Section 1798.130, subdivision (a)(2), states that a business shall respond to requests to know within 45 days of receipt of a verifiable consumer request and that the time may be extended by an additional 45 days. Section 1798.145, subdivision (g), however, states that the period for a business to respond may be extended by up to 90 additional days. This subdivision clarifies that the timing in section 1798.130, subdivision (a)(2), controls. It is better in line with the intent of the CCPA because it ensures that businesses expediently address consumer requests.

Subdivision (c) addresses how businesses are to respond to requests to know personal information. In doing so, it takes a risk-based approach, balancing a consumer's right to know about their personal information collected, used, and shared by a business with the consumer's interest in preventing the disclosure of their personal information to unauthorized persons. The subdivision specifies how a business should respond to requests that seek the disclosure of personal information when the business cannot verify the identity of the consumer, and thereby addresses public concerns raised during the Attorney General's preliminary fact-gathering rulemaking activities.

Subdivision (c)(1) addresses requests that seek the disclosure of specific pieces of personal information and prohibits the business from disclosing specific pieces of personal information when it cannot verify the requestor's identity. **Subdivision (c)(2)**, on the other hand, gives the business discretion to disclose categories of personal information about the consumer when it cannot verify the requestor's identity. In both instances, however, the business must inform the consumer that the business cannot verify their identity. In addition, subdivision (c)(1) requires a business that denies the request for specific pieces of personal information to evaluate whether it can provide categories of personal information instead. Similarly, subdivision (c)(2) requires a business that denies the request for categories of personal information to provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.

These subdivisions are necessary because they describe what a business must do when it cannot readily verify the identity of the consumer. If the business is unable to verify the consumer's identity sufficiently to provide specific pieces of personal information, then it must evaluate whether it can provide categories of personal information. If the business cannot verify the consumer's identity sufficiently to provide categories, then it must respond by providing general information regarding the business's data collection practices. This approach balances the consumer's right to know what personal information a business has about them with the danger of disclosing personal information to unauthorized persons, recognizing that unauthorized disclosure of specific pieces of personal information (for example, a specific medical diagnosis) is frequently more intrusive and harmful to the consumer than the disclosure of mere categories of personal information (for example, medical information).

Subdivision (c)(3) prohibits businesses from providing a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks. **Subdivision (c)(4)** similarly prohibits the business from disclosing a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, health insurance or medical identification number, account password, or security questions and answers. These subdivisions balance the consumer's right to know with the harm that can result from the inappropriate disclosure of information. The subdivisions make clear the instances when a business should not disclose personal information and thereby address public concerns raised during the Attorney General's preliminary rulemaking activities. The subdivisions also reduce the risk that a business will violate another privacy law, such as Civil Code section 1798.82, in the course of attempting to comply with the CCPA.

Subdivision (c)(5) requires a business that denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law or an exception to the CCPA, to inform the requestor and explain the basis for the denial. If the request is denied only in part, the business must disclose the information not subject to the conflict or exception. This subdivision is necessary because it provides direction to businesses on what to communicate to consumers when they deny a request on these grounds. This benefits consumers by giving them greater transparency concerning the business's process for handling their request, and provides them with an opportunity to cure any defects in their request as well as a potential basis for contesting the denial. It also prevents businesses from treating consumers' requests in an all-or-nothing fashion.

Subdivision (c)(6) requires businesses to use reasonable security measures when transmitting personal information to the consumer. This subdivision is necessary to protect consumers' personal information.

Subdivision (c)(7) allows a business that maintains a password-protected account with the consumer to comply with a request to know by utilizing a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information. It requires that the portal fully disclose the personal information that the consumer is entitled to under the CCPA and these regulations, utilize reasonable data security controls, and comply with the verification requirements set forth in these regulations. This subdivision is necessary to provide businesses discretion and flexibility in responding to consumers' requests in a cost-effective

manner while ensuring that businesses comply fully with consumers' requests in a secure fashion. The subdivision does not contravene existing practices that permit consumers to access, delete, or port their personal information. It provides clarity regarding how businesses are to respond to consumer requests, and thereby addresses public concerns raised during the Attorney General's preliminary rulemaking activities.

Subdivision (c)(8) provides that, unless otherwise specified, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request. This subdivision is necessary to provide clarity to businesses regarding when the 12-month "look-back" period referred to in Civil Code section 1798.130, subdivision (a)(2), begins. It responds to questions raised during the Attorney General's preliminary rulemaking activities.

Subdivision (c)(9) requires a business to provide an individualized response to the consumer when responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties. The business may not refer the consumer to the business's general practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories. **Subdivision (c)(10)** further requires a business responding to a verified request to know categories of information to provide for each identified category: (a) the categories of sources from which the personal information was collected; (b) the business or commercial purpose for which it collected the personal information; (c) the categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and (d) the business or commercial purpose for which it sold or disclosed the category of personal information.

These subdivisions are necessary because they provide clarity regarding the business's obligations when responding to requests to know categories of information. They clearly set forth the information that needs to be provided to the consumer. Because the statutory requirements for responding to these requests are distributed throughout the CCPA, pulling them all together and clarifying them in one place makes it easier for businesses, particularly small businesses, to comply. The subdivisions also protect consumers from being denied their right to know by a business responding in a generic and unspecific way.

Subdivision (c)(11) requires that when a business identifies categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, the business must be specific enough to allow consumers a sufficient understanding of the categories listed. This subdivision is necessary to prevent businesses from using generic descriptions that would not properly inform the consumer. The subdivision takes a performance-based approach based on studies of effective privacy notices and plain-language writing. (See Schaub; Center for Plain Language.)

Subdivision (d) addresses how businesses are to respond to requests to delete personal information. **Subdivision (d)(1)** provides that a business that cannot verify the identity of the consumer may deny the request to delete. It further requires the business to inform the requestor that their identity cannot be verified and treat the request as a request to opt-out, pursuant to Civil Code, section 1798.120, subdivision (a). This subdivision is necessary to instruct businesses on what they should do when they cannot verify the identity of the consumer. It addresses concerns

raised by the public during the Attorney General’s preliminary rulemaking activities. In using the word “may,” it gives the business discretion to grant or deny the request. Requiring the business to inform consumers that their identity cannot be verified gives consumers greater transparency into the business’s process for handling their request and provides them with a potential basis for future communication with the business regarding the denial. The subdivision also benefits consumers by requiring the business to view the request in a way that can best accommodate the consumer’s intent to delete the information. When deletion is not possible, requiring a business to treat the request as a request to opt-out of the sale of their personal information benefits the consumer by at least preventing the further proliferation of the consumer’s personal information in the marketplace.

Subdivision (d)(2) specifies that a business shall comply with a consumer’s request to delete their personal information by either: (1) permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems; (2) deidentifying the personal information; or (3) aggregating the personal information.

Subdivision (d)(3) allows a business that stores personal information on archived or backup systems to delay compliance with the consumer’s request to delete, only with respect to data stored on the archived or backup system, until the archived or backup system is next accessed or used. These subdivisions are necessary because they describe how to comply with a consumer’s request to delete and how to handle requests to delete when information is stored on archived or backup systems. It addresses concerns raised during the Attorney General’s preliminary rulemaking activities. Allowing businesses to delete the consumer’s personal information on archived or backup systems at the time that they are accessed or used balances the interests of consumers with the potentially burdensome costs of deleting information from backup systems that may never be utilized.

Subdivision (d)(4) requires the business to specify the manner in which it has deleted the personal information in its response to a consumer’s request to delete. **Subdivision (d)(5)** requires the business to disclose that it will maintain a record of the request pursuant to Civil Code section 1798.105, subdivision (d), in its response to a consumer’s request to delete. These subdivisions are necessary to instruct businesses on what information they must provide to the consumer. They also provide consumers with greater transparency about the business’s practices in deleting personal information.

Subdivision (d)(6) requires businesses that deny a consumer’s request to delete to inform the consumer of the basis for the denial, including any applicable statutory and/or regulatory exception. The business must delete any personal information that is not subject to the exception and not use the consumer’s personal information retained for any other purpose than provided for by the exception. This subdivision is necessary to provide consumers transparency into the business’s practices. It also prevents businesses from using statutory or regulatory exceptions to retain data for their own purposes in derogation of the consumer’s request. It further addresses questions and comments raised by the public during the Attorney General’s preliminary rulemaking activities.

Subdivision (d)(7) allows a business to present the consumer with a choice to delete only select portions of their personal information when responding to a request to delete if a global option to delete all personal information is more prominently presented than the other choices. The business is still required to use the two-step confirmation process set forth in section 999.312,

subdivision (d). This subdivision is necessary to guide businesses on how they can give consumers options for deleting their information. It responds to public comments raised during the Attorney General’s preliminary rulemaking activities about the benefits of providing choices to consumers regarding the deletion of personal information, but also prevents businesses from obfuscating or deemphasizing a global option to delete.

I. 11 CCR § 999.314. Service Providers

The CCPA treats “service providers,” as that term is defined in Civil Code section 1798.140, subdivision (v), differently than businesses. For example, the CCPA does not consider personal information used by or shared with a service provider to perform a business purpose to be a “sale.” (Civ. Code, § 1798.140, subd. (t)(2)(C).) The purpose of section 999.314 of these regulations is to clarify who is a service provider, and how service providers are to handle consumer requests made pursuant to the CCPA. The regulation is necessary to harmonize different parts of the CCPA that have led to confusion regarding how the CCPA applies to service providers. They address concerns raised by the public during the Attorney General’s preliminary rulemaking activities.

Subdivision (a) clarifies that a person or entity providing services to a person or organization that is not a “business” as that term is defined in Civil Code section 1798.140, subdivision (c), but otherwise meets the requirements of a “service provider” under Civil Code section 1798.140, subdivision (v), shall be deemed a service provider for purposes of the CCPA and these regulations. This subdivision is necessary because the definition of “service provider” excludes persons or entities that service non-profit and government entities through its use of the word “business,” which is defined to include only entities “organized or operated for the profit or financial benefit of its shareholders or other owners.” Without this subdivision, entities that process personal information on behalf of non-profit and government entities in accordance with a written contract may be required to comply with consumer requests even when those non-profits and government entities in ultimate control of the information are not required to do so. This unintended and undesired consequence will lead to significant disruption in the functioning of those non-profits and governmental entities and is not in furtherance of the purposes of the CCPA, which clearly excluded non-profits and government entities from being subject to the CCPA. This subdivision addresses concerns raised by the public during the Attorney General’s preliminary rulemaking activities.

Subdivision (b) clarifies that a person or entity that collects personal information directly from a consumer on the business’s behalf that otherwise meets all the other requirements of a “service provider” under Civil Code section 1798.140, subdivision (v), will still be considered a “service provider” for purposes of the CCPA and these regulations. This subdivision is necessary because the definition of “service provider” is incomplete. The CCPA defines “service provider” as an entity that processes information on behalf of a business pursuant to a written contract and “to which the business discloses a consumer’s personal information.” The definition of “business,” however, clearly contemplates entities that collect personal information as directed by or on behalf of a business. (Civ. Code, § 1798.140, subd. (c).) This subdivision clarifies and harmonizes the definition of “business” and “service provider” in furtherance of the purposes of the CCPA and responds to requests to clarify this issue.

Subdivision (c) provides that a service provider shall not use any personal information it received either from a person or entity it services or from the consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity. It does allow, however, service providers to combine personal information received from one or more entities to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity.

This subdivision is necessary because it provides clear guidance regarding the interrelationship of three terms defined in the CCPA: “service provider¹,” “business purpose²,” and “commercial purposes³.” (Civ. Code, § 1798.140, subs. (v), (d), and (f).) A “service provider” is prohibited from using personal information for any purpose other than the “business purpose” specified in the contract it has with the business. The use of personal information for that “business purpose” must be “reasonably necessary and proportionate to achieve the operational purpose” for which it was collected or processed and cannot be used for a “commercial purpose” other than providing the services specified in the contract with the business. It is unclear, however, what is “reasonably necessary and proportionate” when a service provider uses personal information collected from *other* businesses to fulfill the contracted “business purpose” while also promoting and advancing its own commercial interest.

This subdivision clarifies that a service provider’s use of personal information collected from one business to provide services to another business would be outside the bounds of a “necessary and proportionate” use of personal information. Doing so would be advancing the “commercial purposes” of the service provider rather than the “business purpose” of the business. The subdivision, importantly, provides an exception for security and anti-fraud purposes. This exception is consistent with the purposes of the CCPA and with similar exceptions in other California privacy laws. (See Student Online Personal Information Protection Act, Bus. & Prof. Code, § 22584; California Financial Information Privacy Act, Fin. Code, § 4056; Consumer Credit Reporting Agencies Act, Civ. Code, § 1785.15.)

Subdivision (d) requires a service provider that receives and denies a request to know or a request to delete personal information that it handles in its role as a service provider to inform the consumer of the basis for the denial. The basis may include the fact that neither the CCPA

¹ A service provider is defined as a for-profit legal entity “that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, 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.” (Civ. Code, § 1798.140, subd. (v).)

² A “business purpose” is defined as “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.” (Civ. Code, § 1798.140, subd. (d).)

³ “Commercial purposes” is defined as “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,” explicitly excluding engaging in protected free speech. (Civ. Code, § 1798.140, subd. (f).)

nor the regulations require service providers to comply with such requests. The subdivision specifies that the service provider must do so only when it denies the request because there may be situations where a business contractually directs or allows its service provider to comply with such requests.

The subdivision also requires the service provider to inform the consumer that they should make their request directly with the business on whose behalf the service provider maintains the information. If feasible, the service provider shall also provide the consumer with contact information for that business. This subdivision is necessary because it provides clear instructions to service providers on how to respond to consumer requests and benefits consumers by informing them who has control over the personal information that has been collected about them. The subdivision recognizes that service providers may not be contractually allowed to disclose or delete the personal information it handles on behalf of businesses, but in order to facilitate the consumer's request, it instructs service providers to direct the consumer to the business in control of their information. By requiring service providers, when feasible, to provide the contact information of the business it is servicing, the subdivision addresses, in part, concerns raised by the public during the Attorney General's preliminary rulemaking activities that consumers may not know the identity of the companies that have control of personal information about them.

Subdivision (e) clarifies that a service provider that is also a "business," as that term is defined in Civil Code section 1798.140, subdivision (c), shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider. This subdivision is necessary because it provides clear guidance on how entities that are both a service provider and a business are to handle consumer requests and other obligations under the CCPA. It addresses concerns raised by the public during the Attorney General's preliminary rulemaking activities.

J. 11 CCR § 999.315. Requests to Opt-Out

Civil Code section 1798.120, subdivision (a), provides consumers with the right to direct a business that sells personal information about the consumer to third parties to stop selling that information (*i.e.*, request to opt-out). Civil Code section 1798.135, subdivision (a), further requires a business to follow certain requirements with regard to the consumer's right to opt-out, such as providing a "Do Not Sell My Personal Information" link on its webpage and respecting the consumer's decision to opt-out for at least 12 months, among other things. The purpose of section 999.315 of these regulations is to set forth the rules and procedures businesses must follow regarding requests to opt-out made pursuant to Civil Code sections 1798.120 and 1798.135. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(4), requires the Attorney General to establish rules and procedures to facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information and to govern business compliance with a consumer's opt-out request. Section 1798.140, subdivision (i), also requires the Attorney General to approve "designated methods for submitting requests" under the CCPA.

Subdivision (a) requires a business to provide two or more designated methods for submitting requests to opt-out, including an interactive webform accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business's

website or mobile application. It also identifies other acceptable methods for submitting these requests. This subdivision is necessary because Civil Code section 1798.135 only identifies how businesses with an online presence are to comply with Section 1798.120. It does not address other types of business situations. This subdivision requires businesses, whether or not they have a website, to identify at least two methods for submitting requests to opt-out, as they are required to do for requests to know and request to delete. This benefits both the business and consumers by simplifying the procedure, which will in turn allow more consumers to exercise their right to opt-out. In allowing for the shortened phrase, “Do Not Sell My Info,” the subdivision provides businesses some flexibility when designing the opt-out link, such as when it will be viewed on smaller screens, without substantially changing the meaning of the phrase.

Subdivision (b) requires a business to consider several factors—the manner in which the business sells personal information to third parties, available technology, and ease of use by the average consumer—when determining which methods consumers may use to submit requests to opt-out. At least one method offered must reflect the manner in which the business primarily interacts with the consumer. This subdivision is necessary because it prevents businesses from picking obscure methods for submitting requests as a way of discouraging consumers from exercising their right.

Subdivision (c) requires a business that collects personal information online to treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request to opt-out for that browser or device, or, if known, for the consumer. This subdivision is intended to support innovation for privacy services that facilitate the exercise of consumer rights in furtherance of the purposes of the CCPA. This subdivision is necessary because, without it, businesses are likely to reject or ignore consumer tools.

Subdivision (d) allows a business responding to a request to opt-out to present the consumer with the choice to opt-out of the sale of certain categories of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices. This subdivision is necessary because it provides clear guidance regarding how businesses can give consumers choices for opting out of the sale of their information. It responds to public input that providing choices to consumers regarding what personal information can be sold may be beneficial to both consumers and businesses, but also prevents businesses from obfuscating or deemphasizing a global option to opt-out of sale of all personal information.

Subdivision (e) requires a business to act upon a request to opt-out as soon as feasibly possible, but no later than 15 days from the date the business receives the request. This subdivision is necessary because the CCPA is silent on when the business must comply with the request. The subdivision provides clarity for businesses and promotes timely action for consumers exercising their right.

Subdivision (f) requires a business to notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. It also requires the business to inform the consumer when this has been completed. This subdivision is necessary to further the purposes of the CCPA in giving consumers control over the sale of their personal information and to address, in part, concerns raised by the public during

the Attorney General's preliminary rulemaking activities that consumers may not know the identity of the companies to whom businesses have sold their information in order to make an independent request.

In order to exercise the right to opt-out of the sale of their personal information, a consumer must know which businesses hold their information. The realities of today's data-driven marketplace leave most consumers ignorant about what information is being collected about them, who is collecting it, what is being inferred from it, how it is being used, and with whom it is being shared. Consumers may know the business they have a direct relationship with, but they rarely know the identities of the businesses with whom that business shared their personal information. Because the CCPA only requires businesses to disclose the categories of third parties with whom it sold the consumer's information, and not their specific identities, this subdivision places the onus on the business to forward the consumer's request to those businesses that it sold their information within the 90 days prior to receiving the consumer's request. The 90-day look-back period in subdivision (e) is a reasonable time period that balances the business's burden of identifying and contacting the third parties with the consumer's interest in stopping the flow of their information in the marketplace. The requirement to notify the consumer when the business has completed contacting the relevant third parties is necessary to provide the consumer confirmation that the business completed the task. It benefits consumers by giving them greater transparency regarding this process.

Subdivision (g) specifies that a consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission to do so. It provides that a business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer's behalf. It further explains that user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent. This subdivision is necessary to provide clarity on how an authorized agent can make a request to opt-out on behalf of a consumer and what a business may do to obtain proof that the agent is authorized to act on the consumer's behalf. It provides businesses flexibility to require proof, but does not mandate additional record-keeping obligations. The subdivision's provisions on technological tools that signal the consumer's choice to opt-out dispel any potential interpretation that such tools serve as an authorized agent, thus requiring additional proof. This is necessary to prevent businesses from using verification of agency as a means to discourage a consumer from effectively exercising the right to opt-out. It also encourages the development of technological tools to facilitate consumer control.

Subdivision (h) clarifies that requests to opt-out pursuant to Civil Code sections 1798.120 and 1798.135, unlike requests to know and requests to delete, do not need to be verified. The subdivision provides, however, that a business with a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent may deny the request. In those instances, the business must inform the requesting party why it believes the request is fraudulent. This subdivision addresses public comments raised during the Attorney General's preliminary rulemaking activities. The subdivision is based on the fact that the CCPA does not explicitly require requests to opt-out to be verified. Indeed, commenters stressed the importance of a minimally burdensome verification procedure to foster the use of privacy services that empower consumers. The subdivision, however, recognizes that there may be potential for abuse, and thus,

allows businesses to deny requests that they believe are fraudulent as long as they inform the consumer and document their good-faith and reasonable belief.

K. 11 CCR § 999.316. Requests to Opt-In After Opting Out of the Sale of Personal Information

The purpose of section 999.316 of these regulations is to set forth the rules and procedures businesses must follow when a consumer who has opted out of sale of their personal information seeks to reverse that decision. While the CCPA provides consumers with the right to opt-out and requires businesses to respect the consumer's decision to opt-out for at least 12 months, it is silent regarding how a consumer may opt back into the sale of their personal information. This regulation is necessary because Civil Code section 1798.185, subdivision (a)(4), requires the Attorney General to establish rules and procedures to facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information and to govern business compliance with a consumer's opt-out request. Relatedly, businesses and consumers require guidance about how a consumer may opt-in to the sale of their personal information after previously deciding not to do so.

Subdivision (a) requires that requests to opt-in to the sale of personal information use a two-step opt-in process whereby the consumer first, clearly requests to opt-in, and then second, separately confirms their choice. This subdivision is necessary because it provides consumers the opportunity to correct an accidental choice to opt back into the sale of their personal information. It also provides businesses additional assurance that the consumer has made a clear choice to exercise their right to opt-in. This subdivision applies to adults and to minors 13 or older, while section 999.330 of these regulations addresses the opt-in process for minors under the age of 13.

Subdivision (b) allows business to inform a consumer who has opted-out of the sale of personal information that a transaction requires the sale of their personal information as a condition of completing the transaction, and to provide the consumer with instructions on how they can opt-in. This subdivision is necessary because Civil Code section 1798.135, subdivision (a)(5), requires a business to respect the consumer's decision to opt-out for at least 12 months before requesting that they authorize the sale of the consumer's personal information. This subdivision clarifies that a business may inform a consumer who has opted-out of the sale of personal information when the sale of personal information is required to complete a transaction, even if the required 12 months have not passed.

L. 11 CCR § 999.317. Training; Record-Keeping

While the CCPA requires businesses to comply with consumer requests made pursuant to the law and to ensure that all individuals responsible for handling those requests are informed of the CCPA's requirements and how to direct those requests, it is silent on any specific training or record-keeping requirements. The purpose of section 999.317 of these regulations is to clarify and make specific the rules and procedures businesses must follow regarding the training of their staff and the records they must maintain to demonstrate compliance with the CCPA. The regulation is necessary to provide guidance to businesses on how to comply with the law. It also addresses concerns raised by the public during the Attorney General's preliminary rulemaking activities.

Subdivision (a) requires all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA to be informed of all the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations. This subdivision is necessary because Civil Code sections 1798.130, subdivision (a)(6), and 1798.135, subdivision (a)(5), only require individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA to be informed of some of the sections of the CCPA. It omits other relevant sections of CCPA, including 1798.100 and 1798.105, as well as these regulations. This subdivision clarifies that the individuals responsible for handling consumer inquiries about the CCPA and the business's privacy practices know all aspects of the CCPA and these regulations and not just portions of it, which benefits consumers and their ability to exercise their rights.

Subdivision (b) requires that a business maintain records of consumer requests made pursuant to the CCPA, and of how the business responded to said requests, for at least 24 months.

Subdivision (c) allows the records to be maintained in a ticket or log format so long as it includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. This subdivision is necessary to specify the duration and type of information businesses must retain to demonstrate compliance with the CCPA. It balances the principle of data minimization with the need to maintain records to prove compliance, and it assists in the enforcement of the law. It addresses questions regarding record-keeping raised during the Attorney General's preliminary rulemaking activities and benefits businesses by giving them clear direction on how to comply with the law.

Subdivision (d) provides that a business's maintenance of information for record-keeping purposes, where that information is not used for any other purpose, does not by itself violate the CCPA or these regulations. This subdivision is necessary because the public has expressed confusion regarding how to balance the need to prove compliance with the CCPA with consumer requests to delete personal information. This subdivision clarifies that maintaining information for record-keeping purposes is not a violation of the CCPA as long as the information is not used for any other purpose.

Subdivision (e) prohibits businesses from using information maintained for record-keeping purposes for any other purpose. This subdivision is necessary to prevent businesses from using record-keeping as an excuse to use personal information for other purposes.

Subdivision (f) provides that, aside from this record-keeping purpose, a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA. This subdivision is necessary to clarify businesses' obligations under the CCPA. It supports the principle of data-minimization and addresses concerns raised during the Attorney General's preliminary rulemaking activities that a business may be required to retain personal information in order to respond to consumer requests.

Subdivision (g) requires a business that alone or in combination, annually buys, collects for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, to compile and disclose in their privacy policy, the following metrics for the previous calendar year:

- a. the number of requests to know that the business received, complied with in whole or in part, and denied;
- b. the number of requests to delete that the business received, complied with in whole or in part, and denied;
- c. the number of requests to opt-out that the business received, complied with in whole or in part, and denied; and
- d. the median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

It further requires the business to establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the CCPA are informed of all the requirements in the CCPA and these regulations.

This subdivision is necessary to inform the Attorney General, policymakers, academics, and members of the public about businesses' compliance with the CCPA. It considers the burden on businesses to compile and post this information by limiting the requirement to those businesses that handle a large amount of personal information, specifically, the personal information of approximately 10% of California's total population or more. The requirement to establish, document, and comply with a training policy ensures that businesses that are most likely to receive consumer requests because they handle the personal information of a significant portion of California's population are capable of adequately responding to those requests.

M. 11 CCR § 999.318. Requests to Access or Delete Household Information

Civil Code section 1798.140, subdivision (o)(1), defines personal information to include information that could reasonably be linked with a household. Accordingly, consumer requests to know, delete, and opt-out may implicate information related not only to individual consumers, but consumers residing in the same household. The purpose of section 999.318 of these regulations is to clarify and make specific how businesses are to handle requests to access and delete household information. This regulation is necessary because there is a significant amount of public concern and confusion regarding household information. The CCPA does not specify who may access household information and what is required to obtain such information. Additionally, both consumers and businesses have raised concerns during the Attorney General's preliminary rulemaking activities about the disclosure of household information to unauthorized individuals.

Subdivision (a) provides that where a consumer does not have a password-protected account with a business, the business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4. This subdivision is necessary because it clarifies that businesses receiving requests seeking household information outside of the context of a password-protected account shall only provide aggregate household information. This balances the consumer's right to know household information, including household information that the consumer may already be able to access without the CCPA's framework, with the risk of disclosing individualized personal information to an unauthorized person. The subdivision exempts situations involving password-protected accounts so that it does not disrupt existing

procedures businesses may have for accountholders to access non-aggregate household information.

Subdivision (b) provides that if all consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information, and the business can individually verify all the members of the household subject to verification requirements set forth in Article 4, the business shall comply with the request. This subdivision is necessary because it sets forth the requirements businesses must meet to provide specific pieces of information about the household. It balances the consumer's right to this information with the risk that the disclosure would harm individuals within the household.

N. 11 CCR § 999.323. General Rules Regarding Verification

The purpose of section 999.323 of these regulations is to provide guidance to businesses on how to verify that the person making requests to know and requests to delete is the consumer about whom the business has collected information. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(7), requires the Attorney General to establish rules and procedures to govern a business's determination that a request for information received from a consumer is a verifiable consumer request. The Attorney General is required to address the verification of a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account, as well as situations where the consumer does not maintain an account with the business. Section 999.323 of these regulations provides businesses general guidance to apply regarding verification regardless of whether they have a password-protected account with the consumer.

Subdivision (a) requires a business to establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information. This subdivision is necessary because it clarifies that businesses have the responsibility to establish a reasonable method for verifying the identity of the person making the request. The business must also document and comply with the method that it establishes. The subdivision provides businesses with a significant amount of discretion and flexibility to select a workable method while still setting a baseline requirement that the method be "reasonable." Requiring the documentation of the method also provides transparency into the process and an easy way to confirm that the business has set up a method and is following it. Additional subdivisions explained below set forth further principles the business must comply with when verifying a consumer request.

Subdivision (b) sets forth principles businesses must follow in determining the method by which they will verify consumers' identities. **Subdivision (b)(1)** requires a business to, whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service. **Subdivision (b)(2)** requires a business to avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purposes of verification. **Subdivision (b)(3)** requires a business to consider a variety of factors in determining the verification method, such as the type, sensitivity, and value of the personal information collected and maintained, the risk of harm posed by any unauthorized access or deletion, the likelihood that fraudulent or malicious actors seeking the information, whether the

information can be spoofed, the manner in which the business interacts with the consumer, and available technology for verification.

These subdivisions are necessary to provide clear guidance to businesses on what they should consider when determining a verification method. Because businesses have a significant amount of flexibility to determine how to verify, these subdivisions provide principles that illustrate what the baseline “reasonable” requirement includes. They also support data minimization principles and prevent businesses from using verification as an excuse to collect sensitive personal information.

Subdivision (c) requires businesses to generally avoid requesting additional information from the consumer for purposes of verification. It allows businesses to request additional information from the consumer if they cannot verify the identity of the consumer with the information they already have, but restricts them from using that information for any purpose other than verification or security or fraud-prevention. It further requires a business to delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer’s request, except as required by section 999.317 of these regulations. This subdivision is necessary to support data minimization principles. It protects consumers by prohibiting businesses from using verification as an excuse to collect and use personal information for other means.

Subdivision (d) requires a business to implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer’s personal information. This subdivision is necessary to clarify that businesses are held to reasonable data security practices when verifying users whether or not the user maintains an account with the business. Because section 999.324 of these regulations gives businesses a significant amount of deference when they have an existing password-protected account with the user, this subdivision is necessary to ensure that businesses implement reasonable data security measures within that password-protected account framework.

Subdivision (e) provides that a business that maintains deidentified consumer information does not have to provide or delete the deidentified information in response to a consumer request or re-identify individual data to verify a consumer request. This subdivision is necessary because it responds to questions raised during the Attorney General’s preliminary rulemaking activities. The subdivision makes clear that the CCPA does not apply to deidentified or aggregated consumer information or require businesses to re-identify or otherwise link information that would not be considered personal information. (Civ. Code, §§ 1798.145, subd. (a)(5), 1798.145, subd. (i).)

O. 11 CCR § 999.324. Verification for Password-Protected Accounts

The purpose of section 999.324 of these regulations is to provide further guidance to businesses on how to verify that the person making requests to know and requests to delete is the consumer about whom the business has collected information. Section 999.324 specifically provides businesses guidance to apply regarding verification when the consumer has a password-protected account with the business. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(7), requires the Attorney General to establish rules and procedures to govern a business’s determination that a request for information received from a consumer is a verifiable consumer request.

Subdivision (a) allows a business that maintains a password-protected account with the consumer to verify the consumer's identity through the business's existing authentication practices for the consumer's account if the business uses reasonable security measures to protect the account and follows the requirements in section 999.323 of these regulations. The subdivision also requires consumers to re-authenticate themselves before the disclosure or deletion of the consumer's data. This subdivision is necessary to fulfill the requirements of Civil Code section 1798.185, subdivision (a)(7), with regard to password-protected accounts. It gives businesses a significant amount of flexibility to utilize their existing verification processes while still holding them to reasonable data security standards to ensure that consumers are protected from fraudulent activity. The subdivision's requirement that consumers re-authenticate themselves is an additional security measure to protect the consumer from unauthorized access adopted from public input during the Attorney General's preliminary rulemaking activities.

Subdivision (b) prohibits a business that suspects fraudulent or malicious activity on or from the password-protected account from complying with a consumer's request to know or request to delete until further verification procedures determine otherwise. The subdivision also identifies the procedures set forth in section 999.325 of these regulations as a way to verify the identity of the consumer. This subdivision is necessary to protect consumers from the unauthorized access to or deletion of their personal information. It benefits businesses by providing clear direction that the business should prioritize security and fraud-prevention over disclosure, but also benefits consumers by requiring the business to undertake further verification measures and by providing guidance regarding what those further measures could be.

P. 11 CCR § 999.325. Verification for Non-Accountholders

The purpose of section 999.325 of these regulations is to provide further guidance to businesses on how to verify that the person making requests to know and requests to delete is the consumer about whom the business has collected information. Section 999.325 specifically provides businesses with guidance regarding verification when the consumer does not have a password-protected account with the business. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(7), requires the Attorney General to establish rules and procedures to govern a business's determination that a request for information received from a consumer is a verifiable consumer request.

Subdivision (a) requires a business that does not have a password-protected account with the consumer to comply with subsections (b) through (g) in this section in addition to section 999.323 of these regulations. This subdivision is necessary to clarify which regulations apply to businesses that do not have a password-protected account with the consumer.

Subdivision (b) requires a business complying with a request to know categories of personal information to verify the identity of the consumer making the request to a reasonable degree of certainty. It further provides that a reasonable degree of certainty may include matching at least two data points provided by the consumer with the data points maintained by the business. This subdivision is necessary to set a clear standard—reasonable degree of certainty—businesses must meet when verifying a request to know categories of personal information when they do not have an account with the consumer. The subdivision also provides guidance on how the business may meet that standard.

Subdivision (c) requires a business responding to a request to know specific pieces of personal information to verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. Subdivision (c) defines a reasonably high degree of certainty to be the matching of at least three pieces of personal information provided by the consumer with personal information maintained by the business together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Subdivision (c) further requires businesses to maintain all signed declarations as part of their record-keeping obligations.

This subdivision is necessary to set a standard—reasonably high degree of certainty—businesses must meet when processing a request to know specific pieces of personal information when they do not have an account with the consumer. It benefits businesses by setting forth objective ways in which a consumer can meet this higher bar for verification. It also instructs businesses on what records they must retain to demonstrate compliance with this regulation. The record-keeping requirement balances the consumer’s right to know and delete with the need to protect consumers from the unauthorized disclosure or deletion of their personal information. Requiring a declaration signed under penalty of perjury gives consumers a way to verify their identity, but also allows legal recourse against a person submitting a fraudulent request.

Subdivision (d) requires a business complying with a request to delete to act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with the regulations set forth in Article 4. It allows a business to verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require a reasonable degree of certainty. This subdivision is necessary to provide businesses guidance regarding the standard they should apply when verifying requests to delete. It also provides businesses flexibility in determining whether to use a reasonable degree or a reasonably high degree of certainty, but also holds them accountable for making a good-faith determination. The subdivision also gives guidance to businesses by providing an example of when a business may require a lower or higher standard for verification.

Subdivision (e) provides illustrative examples of how to verify non-accountholders. The first example addresses a situation where a business has personal information associated with a named actual person such as a consumer’s name and credit card number. It explains that the business could verify the consumer by asking for the credit card security code and recent purchases made with the credit card. The second example addresses a situation where personal information is not associated with a named actual person. It explains that the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information and that the business may be required to conduct a fact-based verification process that considers the factors set forth in section 999.323, subdivision (b)(3), of these regulations.

This subdivision is necessary to guide businesses on how to verify the identity of a consumer requesting information when they do not maintain an account with the business. These examples provide sample acceptable methods for verification and underscore that businesses are capable of verifying non-accountholders based on existing data collected from these consumers.

Subdivision (f) requires a business to inform the consumer in response to any request to know or request to delete that it receives if there is no reasonable method by which it can verify the consumer's identity to the degree of certainty required. If there is no reasonable method to verify the consumer's identity to the degree of certainty required for all the personal information the business holds, this subdivision requires the business to disclose in its privacy policy why there is no reasonable method. The subdivision further requires the business to evaluate and document on a yearly basis whether a method can be established.

This subdivision is necessary because it acknowledges that there may be instances where a consumer's identity cannot be verified to the standard required by these regulations. The business, however, must still evaluate and document on a yearly basis whether a reasonable method can be established in the event that new technologies or methods are available to adequately verify the consumer. The yearly evaluation and explanation within the business's privacy policy ensures that businesses are complying with the regulation and provides transparency in the business's processes. It also informs the Attorney General, policymakers, academics, and members of the public of situations where verification is an impediment to a consumer's ability to exercise their rights.

Q. 11 CCR § 999.326. Authorized Agent

The CCPA allows consumers to authorize another person to make requests to businesses on their behalf. (Civ. Code, §§ 1798.135, subs. (a)(1), (c), 1798.140, subd. (y), 1798.185, subd. (a)(7).) The purpose of section 999.326 of these regulations is to provide guidance to businesses regarding how to handle requests made by an authorized agent of the consumer. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(7), requires the Attorney General to establish rules and procedures to facilitate a consumer's authorized agent's ability to obtain information pursuant to the CCPA. It benefits businesses by guiding them in how to structure their procedures for handling consumer requests through an agent, and it benefits consumers by setting the ground for innovation and the development of new technology in this area, which will allow them increased opportunities to exercise their rights under the CCPA.

Subdivision (a) allows a business to require consumers who use an authorized agent to submit a request to know or delete on their behalf to provide the authorized agent with written permission to do so, and to require consumers to verify their identity directly with the business. This subdivision is necessary to instruct businesses what they may require of consumers who use an authorized agent to make a request on their behalf. It gives businesses discretion to require written proof of authorization and verification of identity directly from the consumer. Requiring the consumer to verify their identity directly with the business allows businesses to utilize their existing verification processes and complies with general privacy principles to not share one's security credentials (login ID and passwords) with others. Authorized agents will serve to facilitate requests and responses, but they themselves will not be allowed to collect or amass consumers' sensitive information for the purposes of verification. Discretion is given to the business because the business may determine, based on the factors set forth in section 999.323, subdivision (b), of these regulations that such requirements are unwarranted.

Subdivision (b) clarifies that subdivision (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465. This subdivision is necessary because agents with the consumer's power of attorney either are acting

in their place with clear explicit consent or because the consumer is incapacitated. In those instances, the consumer should not be required to authenticate their identity directly with the business. The agent shall act in accordance with established laws concerning powers of attorney.

Subdivision (c) provides that a business may deny a request from an agent that does not submit proof that it has been authorized by the consumer to act on the consumer's behalf. This subdivision is necessary to clarify that businesses may deny requests from agents that do not submit proof that they have been authorized by the consumer to act on their behalf either through the requirements of section 999.326, subdivision (a) or (b).

R. 11 CCR § 999.330. Minors Under 13 Years of Age

Civil Code section 1798.120, subdivision (c), prohibits a business that has actual knowledge that it has personal information of a consumer under the age of 13 from selling that information unless the consumer's parent or guardian has affirmatively authorized the sale, referred to as the "right to opt-in" to sale. The purpose of section 999.330 of these regulations is to set forth the rules and procedures businesses must follow with regard to the personal information of children under the age of 13. This regulation is necessary to instruct businesses on how to implement a process for a parent or guardian to opt-in to the sale of personal information of their child under the age of 13.

Subdivision (a)(1) requires a business that has actual knowledge that it collects or maintains the personal information of children under the age of 13 to establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. The requirement of a "reasonable method" is based on the similar requirement in the Children's Online Privacy Protection Act (hereinafter COPPA) (15 U.S.C. § 6501, *et seq.*) This subdivision is necessary because the CCPA does not specify how a parent or guardian is to affirmatively authorize the sale of a child's personal information. Requiring the documentation of the method also provides transparency into the process and an easy way to confirm that the business has set up a method and is following it.

The subdivision also requires that the affirmative authorization by the parent or guardian be in addition to any verifiable parental consent required under COPPA, which only covers personal information collected online *from* a child under the age of 13. This is necessary because the CCPA's prohibition on the sale of children's personal information covers information regardless of whether collected online, offline, or from a third party.

Subdivision (a)(2) provides various methods that are reasonably calculated to ensure that the person providing the required consent is the child's parent or guardian. The methods are the same as those set forth in regulations issued by the Federal Trade Commission in furtherance of COPPA, which have been tested and used for over twenty years. This subdivision is necessary to provide guidance to businesses on how to verify the identity of a parent or guardian.

Subdivision (b) requires a business that receives an affirmative authorization pursuant to subdivision (a) of this section to inform the parent or guardian that they can opt-out of the sale of their child's personal information at a later time. The business must also inform them of the process for doing so. This requirement is necessary to ensure that the parent or guardian is aware of their right to opt-out and the procedure to do so. This is particularly important in the case of a

business that directs its products or services to children under the age of 13 and does not sell their personal information without affirmative authorization because such a business would not otherwise be required to provide an opt-out notice, pursuant to section 999.332, subdivision (b), of these regulations.

S. 11 CCR § 999.331. Minors 13 to 16 Years of Age

Civil Code section 1798.120, subdivision (c), prohibits a business with actual knowledge that it has personal information of a minor 13 to 16 years of age from selling that information unless the minor has affirmatively authorized the sale, referred to as the “right to opt-in” to sale. The purpose of section 999.331 of these regulations is to set forth the rules and procedures businesses must follow with regard to the personal information of minors at least 13 and less than 16 years of age. This regulation is necessary to instruct businesses on how to implement the process for such minors to opt-in to the sale of their personal information. It also clarifies that this regulation applies to minors at least 13 and less than 16 years of age. This clarification is necessary because Civil Code section 1798.120, subdivision (c), uses both the phrases “less than 16 years of age” and “between 13 and 16 years of age,” which creates some ambiguity as to whether the right to opt-in applies to minors 16 years of age.

Subdivision (a) requires a business that has actual knowledge that it collects or maintains the personal information of minors at least 13 and less than 16 years of age to establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information, pursuant to section 999.316 of these regulations. This subdivision is necessary because the CCPA does not specify how a business is to implement the process for minors to opt-in to the sale of their personal information. Requiring the documentation of the method also provides transparency into the process and an easy way to confirm that the business has set up a method and is following it.

Subdivision (b) requires a business that receives a request to opt-in to the sale of personal information from a minor at least 13 and less than 16 years of age to inform the minor that they have the right to opt-out of the sale of their personal information at a later time. The business must also inform them of the process for doing so. This requirement is necessary to ensure that consumers at least 13 and less than 16 years of age are aware of their right to opt-out and the procedure to do so. This is particularly important in the case of a business that directs its products or services to children under the age of 16 and does not sell their personal information without affirmative authorization because such a business would not otherwise be required to provide an opt-out notice, pursuant to section 999.332, subdivision (b), of these regulations.

T. 11 CCR § 999.332. Notices to Minors

Civil Code section 1798.120, subdivision (c), prohibits businesses from selling the personal information of minors less than 16 years of age without their affirmative authorization or, in the case of children under the age of 13, the affirmative authorization of a parent or guardian. The law implicitly requires a business with actual knowledge that it has the personal information of such minors to notify them of the right and the procedure for affirmatively authorizing the sale of their personal information. The purpose of section 999.332 of these regulations is to set forth the rules and procedures businesses must follow regarding notices to consumers under the age of 16.

The regulation is necessary to further the CCPA’s purposes in providing special protections for the personal information of minors.

Subdivision (a) requires a business that is subject to sections 999.330 and 999.331 of these regulations to include a description of the processes set forth in those sections in its privacy policy. The subdivision is necessary to implement Civil Code section 1798.120, subdivision (b), and to instruct businesses on what information they must disclose to consumers.

Subdivision (b) clarifies that businesses exclusively targeting offers of goods or services directly to consumers under 16 years of age that do not sell the personal information of said consumers without their affirmative authorization do not need to provide a notice of right to opt-out. The subdivision is necessary to prevent consumer confusion because the inclusion of a right to opt-out, for example through a website link saying “Do Not Sell My Personal Information,” may cause minors or their parents or guardians to mistakenly assume that the business sells their personal information unless they took action. This subdivision responds to concerns raised during the Attorney General’s preliminary rulemaking activities.

U. 11 CCR § 999.336. Discriminatory Practices

Civil Code section 1798.125 prohibits businesses from discriminating against a consumer for the exercise of their rights under the CCPA, but allows a business to offer a financial incentive as long as the value of the incentive is reasonably related to the value provided by the consumer’s data. The purpose of section 999.336 of these regulations is to clarify and provide businesses guidance and instruction regarding the offering of financial incentives. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(6), requires the Attorney General to establish rules and procedures regarding financial incentive offerings. It also responds to questions raised during the Attorney General’s preliminary rulemaking activities. The regulation benefits businesses by providing guidance on how to structure their financial incentive programs, and it benefits consumers by providing transparency into how businesses value their data.

Subdivision (a) explains that a financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, subdivision (a), if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations. This subdivision clarifies that the CCPA only prohibits a financial incentive or price or service difference if it is discriminatory. If there is no difference in treatment between those who have and those who have not exercised their right to know, delete, or opt-out, then this section does not apply. This subdivision is necessary because the public expressed a significant amount of confusion and misunderstanding about this issue during the Attorney General’s preliminary rulemaking activities.

Subdivision (b) explains that a business may offer a price or service difference if it is reasonably related to the value of the consumer’s data as that term is defined in section 999.337 of these regulations. This subdivision is necessary because Civil Code section 1798.125 uses both “reasonably related to” and “directly related to” in referencing the value of the consumer’s data and in describing when the CCPA would allow a business to offer a price or service difference. (Civ. Code, §§ 1798.125, subd. (a)(2) (“if that difference is reasonably related to the value provided to the consumer by the consumer’s data”) and 1798.125, subd. (b)(1) (“if that price or difference is directly related to the value provided to the consumer by the consumer’s data”).)

The public expressed confusion and raised questions regarding which of the two terms controls during the Attorney General’s preliminary rulemaking activities. This subdivision clarifies that the term “reasonably related to the value” controls because it is better in line with the intent of the CCPA to match the price or service difference to the value of the data. “Directly related” could arguably be interpreted broadly to mean any direct correlation to the amount, whereas “reasonably related” would not.

Subdivision (c) provides examples that illustrate the interaction of the two previous subdivisions by identifying the type of incentive offered, the exercise of the privacy right, and the value of the personal information involved. The subdivision is necessary to address confusion regarding the CCPA’s provisions on discrimination. During the Attorney General’s preliminary rulemaking activities, businesses expressed concern about the potential impact of the discrimination provisions of the CCPA on loyalty programs through which they offer consumers rewards for continued patronage. The California Chamber of Commerce and the California Retailers Association urged the Attorney General to exempt loyalty programs from the CCPA. Rather than offering a wholesale exemption, subdivision (c) provides illustrative examples of how a business may design the terms of a financial incentive, such as a loyalty program, to continue to reward customer loyalty, but not trigger CCPA’s prohibition on discrimination.

Subdivision (d) clarifies that a business’s denial of a consumer’s request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations is not considered discriminatory. This subdivision is necessary to distinguish a denial of the exercise of a right for a permitted reason, such as being unable to verify the identity of the consumer as provided in Article 4 of these regulations, from a denial that would constitute discrimination.

Subdivision (e) requires a business to notify consumers of any financial incentive or price or service difference it offers subject to Civil Code section 1798.125 and to do so in accordance with the notice provisions set forth in section 999.307 of these regulations. This subdivision implements Civil Code section 1798.125, subdivision (b)(2), and is necessary to ensure that businesses give consumers information to assist them in making decisions on financial incentive offerings that implicate their personal information. The subdivision allows a business to provide a separate notice, rather than mandating disclosure in a privacy policy, because businesses may offer financial incentives at different times and with varying terms for different consumers.

Subdivision (f) clarifies that the charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (g)(3), is not a financial incentive subject to these regulations. This subdivision is necessary to clarify a potential point of confusion regarding the interaction of various sections of the CCPA.

V. 11 CCR § 999.337. Calculating the Value of Consumer Data

Civil Code section 1798.125 requires financial incentives that implicate a consumer’s privacy rights to be both “directly related to the value” and “reasonably related to the value” of the consumer’s data. The purpose of section 999.337 of these regulations is to clarify and establish methods by which a business may calculate the value of consumer data in designing and disclosing financial incentive offerings that are not discriminatory. This regulation is necessary because the statute provides no method for calculating the value of consumers’ data. It benefits both consumers and businesses by specifying various methods a business may use to make the required calculation.

Subdivision (a) explains that the value provided to the consumer by the consumer's data, as that term is used in Civil Code section 1798.125, is the value provided to the business by the consumer's data. It further explains that the regulations refer to this term as "the value of the consumer's data."

This subdivision is necessary to remove any confusion about a possible distinction between the value of a consumer's data to a business and the value of the data to the consumer. Studies have found that there is not a single generally accepted methodology for calculating the value of a consumer's data, whether to a business or to a consumer. One study found that the majority of the 36 companies that they studied with annual revenue over \$1 billion did not have formal data valuation practices and that "there is no formula for placing a precise price tag on data." (Short et al., *What's Your Data Worth?* (Mar. 3, 2017) MIT Sloan Management Review, Spring 2017 Issue.) Another study found that the number of businesses in the market for data significantly affects the value of consumers' data to businesses. (Montes et al., *The value of personal information in markets with endogenous privacy* (Aug. 5, 2015) CEIS Working Paper No. 352.) Another group of researchers studied consumers' valuation of their own data and found that they assigned markedly different values depending on context, concluding that such subjective valuation is unlikely to provide a sufficient basis on which to estimate the value of data. (Acquisti et al., *What Is Privacy Worth?* (2013) *The Journal of Legal Studies*, 42(2), pp. 249-274; Spiekermann, et al., *Towards a Value Theory for Personal Data* (April 2017) *Journal of Information Technology*, Vol. 32, Issue 1, 2017.)

Accordingly, this subdivision sets forth the standard by which businesses must determine value of the customer's data as the value provided to the business by the consumer's data. It chooses to use an objective calculation (to be demonstrated in accordance with subdivision (b) of this regulation), as opposed to a consumer's subjective estimation of the value of their data. This benefits businesses by allowing uniformity in the offering of financial incentives. The regulation's defining of the term "the value of the consumer's data" also makes the regulation more readable, and thus, easier for consumers and businesses to understand.

Subdivision (b) requires a business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 to use and document a reasonable and good faith method for calculating the value of the consumer's data. The subdivision is not prescriptive. Rather, it provides eight methods by which the business shall calculate the value of the consumer's data, including a catchall "any other practical and reliable method of calculation used in good faith." Documentation of the calculation facilitates the Attorney General's ability to investigate whether the financial incentive is reasonably related to the value of the data, and benefits both businesses and consumers by increasing businesses' accountability to the law.

The methods provided are based on comments received during the Attorney General's preliminary rulemaking activities, a review of the academic literature cited above, and internal discussion and research. As noted, there is no one established consensus method for calculating the value (e.g., from the sale, collection, or retention) of a consumer's data. Accordingly, the subdivision allows businesses discretion in finding an approach that best suits their industry and business practices. It also allows the Attorney General's Office to learn over time from the use of different approaches, including for purposes of enforcement.

The methods build on a number of concepts and considerations. One concept is the difference between marginal and average value, economic concepts helpful for understanding the value of a

consumer's data. The average value of a consumer's data, used in subdivision (b)(1), is the total value of all consumers' data divided by the total number of consumers. Marginal value, used in subdivision (b)(2), is the additional value a business earns from adding just one more consumer's data. The marginal value of a consumer's data is likely to be less than the average value because adding (or subtracting) one more consumer's information to a data portfolio containing the data of a large number of consumers is unlikely to change the value of that portfolio significantly. In contrast, dividing the total value of a portfolio containing many consumers' data by the total number of consumers may yield a much higher average value than the marginal value of a single consumer's data.

Allowing businesses to use the marginal value of a consumer's data in setting the value of a financial incentive would benefit consumers because then the cost of financial incentive would be lower. Prescribing businesses, however, to use the marginal value in calculating the value of a consumer's data may be burdensome to businesses, particularly small businesses, who do not have the resources to make those calculations. A marginal value calculation would require a new estimate every time a new consumer enters or exits the data pool. Furthermore, because businesses may buy, sell, and use data in bulk, they may have no way to assess how the value of that data would change if a single consumer left the pool. Accordingly, this subdivision allows businesses to use either method of calculation.

As an alternative, subdivisions (b)(3) through (b)(7) recognize that businesses may value consumer's data in different ways. These subdivisions allow businesses to calculate the value of a consumer's data by relying on concepts of revenue, expenses, and profit. While businesses may track these factors in different ways, these factors may collectively influence the value of a consumer's data to the business. Profit from the sale, collection, or retention of consumers' data may be the most direct gauge of the value of a consumer's data, but many businesses may not know what portion of their profit derives from consumers' data. This is because some revenue and expenses align with both data-related and non-data-related activities (*e.g.*, cost of servers that house consumer data and other data, revenue from total sales that captures sales in a discounted loyalty program and outside the loyalty program). The flexibility provided by these subdivisions allows businesses to select a method that best fits with the way they use consumers' data.

Lastly, subdivision (b)(8) leaves open the possibility of a business departing from the methods listed in the subdivision so long as the calculation method satisfies three criteria: it must be practical, reliable, and used in good-faith. In addition, recognizing that some businesses may not have the ability to calculate the value of California consumers' data separately from that of other U.S. consumers, subdivision (b) allows businesses to choose which to use. A business may make the calculation based on the data of either a "consumer," defined in Civil Code section 1798.140, subdivision (g), as "a natural person who is a California resident," or a "typical consumer," defined in section 999.301, subdivision (s), of these regulations as "a natural person residing in the United States."

W. 11 CCR § 999.341. Severability

The purpose of this regulation is to clarify that if any portion of the regulations contained in the Chapter is held to be unconstitutional, contrary to statute, exceeding the authority of the Attorney General, or otherwise inoperative, the remaining portions of the regulations will remain valid.

This regulation is necessary in the event that legal challenges are made to the regulations, and thus, this regulation will clarify what will occur if some of these regulations are deemed invalid.

V. TECHNICAL, THEORETICAL, AND/OR EMPIRICAL STUDIES, REPORTS OR DOCUMENTS

Acquisti et al., *What Is Privacy Worth?* (2013) *The Journal of Legal Studies*, 42(2), pp. 249-274. Available at SSRN: <https://ssrn.com/abstract=3305331>.

California Department of Justice, Attorney General's Office, *California Data Breach Report* (February 2016). Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>.

California Department of Justice, Attorney General's Office, *Public Comments Received as Part of the Preliminary Rulemaking Process*. Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf>.

California Department of Justice, Attorney General's Office, *Supplemental Public Comments Received as Part of the Preliminary Rulemaking Process*. Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/supplemental-public-comments.pdf>.

California Department of Justice, Attorney General's Office, *Transcript of Fresno Public Forum*. Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-fresno-021319.pdf>.

California Department of Justice, Attorney General's Office, *Transcript of Inland Empire/Riverside Public Forum*. Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-riverside-012419.pdf>?

California Department of Justice, Attorney General's Office, *Transcript of Los Angeles Public Forum*. Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-los-angeles-012519.pdf>?

California Department of Justice, Attorney General's Office, *Transcript of Sacramento Public Forum*. Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-sac-020519.pdf>?

California Department of Justice, Attorney General's Office, *Transcript of San Diego Public Forum*. Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-sd-011419.pdf>?

California Department of Justice, Attorney General's Office, *Transcript of San Francisco Public Forum*. Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-sf-010819.pdf>?

California Department of Justice, Attorney General's Office, *Transcript of Stanford Public Forum*. Available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-stanford-030519.pdf>.

Center for Plain Language, *Privacy-policy analysis* (2015). Available at <https://centerforplainlanguage.org/wp-content/uploads/2016/11/TIME-privacy-policy-analysis-report.pdf>.

Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, FTC Report* (March 2012). Available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

Hahn et al., *A data processing addendum for the CCPA?* (Jun. 19, 2019) IAPP Privacy Perspectives <https://iapp.org/news/a/a-data-processing-addendum-for-the-ccpa/?mkt_tok=eyJpIjoiT0RSaU5HSmpaV1V5TWpSbCIiInQoIiwldlRLOStnYUI4d1FsK0VuMVNsR2ZjR1JxZkdSQ3FqOVFFU1hnRmkra0lrWVozdys0UDF0MXNZUmpEZlcyOFdONjFkQ1dNOEJBYnF2NctUTitpSmVyR2h0emlnVnpibnUyNk9YaEFQaXJ4ZmJyeUdlYTUvcmlJGTjRnXC9RcmRMREcifQ%3D%3D> [as of Aug. 7, 2019].

Javelin Strategy & Research, *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt* (March 6, 2019). Available at <https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt>.

Montes et al., *The value of personal information in markets with endogenous privacy* (Aug. 5, 2015) CEIS Working Paper No. 352. Available at SSRN: <https://ssrn.com/abstract=2640177> or <http://dx.doi.org/10.2139/ssrn.2640177>.

National Telecommunications and Information Administration, U.S. Department of Commerce, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* (July 25, 2013). Available at https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model* (2016) 27 *Fordham Intell. Prop. Media & Ent. L.J.* 181. Available at: <https://ir.lawnet.fordham.edu/iplj/vol27/iss1/5>.

Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* (November 14, 2014). Available at https://www.pewresearch.org/wp-content/uploads/sites/9/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation* (March 22, 2016) *Journal of Legal Studies*, Forthcoming; Fordham Law Legal Studies Research Paper No. 2715164. Available at <https://ssrn.com/abstract=2715164> or <http://dx.doi.org/10.2139/ssrn.2715164>.

Schaub, et al., *A Design Space for Effective Privacy Notices* (July 22–24, 2015) Symposium on Usable Privacy and Security (SOUPS) 2015, Ottawa, Canada. Available at <https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub>.

Short et al., *What's Your Data Worth?* (Mar. 3, 2017) *MIT Sloan Management Review*, Spring 2017 Issue. Available at <https://sloanreview.mit.edu/article/whats-your-data-worth/>.

Spiekermann, et al., *Towards a Value Theory for Personal Data* (April 2017) *Journal of Information Technology*, Vol. 32, Issue 1, 2017. Available at SSRN: <https://ssrn.com/abstract=3168528> or <http://dx.doi.org/10.1057/jit.2016.4>.

VI. STANDARDIZED REGULATORY IMPACT ANALYSIS

The standardized regulatory impact analysis (SRIA) and the Department of Finance’s comment letter on the SRIA are attached to this ISOR as Appendix A and B, respectively.

VII. REASONABLE ALTERNATIVES AND THE ATTORNEY GENERAL’S REASONS FOR REJECTING THOSE ALTERNATIVES

The Attorney General considered several alternatives in drafting the proposed regulations. In considering the following alternatives, the Attorney General sought to balance the benefits to consumers, the burden to businesses, and the purposes of the CCPA. The alternatives considered and rejected are below.

A. Sections 999.301, subdivisions (d) and (e) – Definitions of “Categories of Sources” and “Categories of Third Parties”

Alternative: The Attorney General considered and rejected alternative approaches to the definitions for “categories of sources” and categories of third parties. These alternatives included one that would attempt to identify every possible category of sources and third parties, and another hands-off approach that left the terms undefined.

Reasoning: The Attorney General rejected both these alternatives and took a hybrid approach in defining these terms. Identifying as many possible categories of sources and third parties may provide greater transparency for consumers for a certain time period, but it would risk becoming outdated by evolving technologies and business practices. Leaving the terms undefined, on the other hand, would likely result in the sort of vague and confusing language for which privacy policies are frequently criticized today. (See Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FTC Report (March 2012), pp. 60-64 (hereafter Federal Trade Commission); Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model* (2016) 27 Fordham Intell. Prop. Media & Ent. L.J. 181 (hereafter Norton); Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation* (March 22, 2016) Journal of Legal Studies, Forthcoming; Fordham Law Legal Studies Research Paper No. 2715164 (hereafter Reidenberg).) Identifying some categories by name, while also requiring businesses the performance standard of providing notices in a manner that would be “understandable to an average consumer,” balances the need for the regulations to be both specific and flexible to change.

B. Sections 999.305, 999.306, 999.307, and 999.308 – Presentation of Notices

Alternatives: The Attorney General considered and rejected a more prescriptive approach in the format and method by which businesses provide consumers the notices required by the CCPA, including the privacy policy.

Reasoning: Studies have found that the manner of presentation and the use of plain language techniques heavily influence the effectiveness of privacy notices in achieving consumer comprehension. (See Schaub; Center for Plain Language.) Given the wide range of businesses subject to the CCPA, businesses will be providing notices to consumer in a variety of contexts,

both online and offline. The Attorney General reasoned that prescribing the manner and format in which businesses provide notices to consumers may not best facilitate the comprehension of these notices. Thus, the regulations on notice take a performance-based approach, calling for the notices to be designed and presented in a way that makes them easy to read and understandable by consumers, with some specific requirements drawn from the studies to further those ends. The regulation places the onus on the business to determine the best way to communicate the required information and provides them with the flexibility to craft the notices in a way that the consumer understands them.

C. Sections 999.305, subdivision (d) – Notice at Collection

Alternatives: The Attorney General considered and rejected the alternative of allowing businesses that do not collect personal information directly from consumers to rely solely on a signed attestation or contractual assurance from the original source of the personal information that they provided the notice at collection.

Reasoning: The Attorney General rejected the alternative of simply relying on the signed attestation of the original source of the personal information because of concerns raised by the public during preliminary rulemaking activities. Businesses, such as third-party data brokers, that do not collect personal information directly from consumers, may not be in a position to provide a notice at collection to consumers at or before the time of collection, but they are in a position of ensuring that the notice at collection is given correctly. Oftentimes, consumers are unaware of the businesses that sell their personal information. By requiring signed attestations that include a description and example of the notice at collection, not only do consumers have the ability to determine whether they did in fact receive that notice at collection, businesses have the assurance that the source of the information complied with the law. Simply allowing attestations without this additional information would not allow for these internal checks. Moreover, obtaining this additional information should not be overly burdensome since the business would have had to contact the sources to acquire a signed attestation even in the suggested alternative.

D. Section 999.312, subdivisions (a) through (c) – Methods for Submitting Requests to Know and Requests to Delete

Alternative: The Attorney General considered and rejected alternative approaches to Section 999.312, subdivisions (a) through (c), to prescribe specific methods by which consumers may submit their requests to know and requests to delete.

Reasoning: Given the wide variety of different industries subject to the CCPA, there are many different ways in which consumers may interact with businesses subject to the CCPA. Prescribing the method by which consumers submit their requests to know and requests to delete may not best address all the different ways in which consumers interact with businesses. In addition, prescribing a method may not allow flexibility to adapt to evolving technologies and business practices. Accordingly, the Attorney General chose to allow businesses flexibility to determine two methods to offer the consumer while still requiring at least one method to reflect the primary way in which the business interacts with the consumer. This best balances consumers' ability to exercise their rights with the burden on businesses, particularly small businesses, to offer multiple procedures to manage.

E. Section 999.317, subdivision (g) – Training and Record-Keeping

Alternative: The Attorney General considered and rejected alternative approaches to Section 999.317, which establishes a personal information volume threshold for enhanced training and record-keeping requirements. Specifically, the Attorney General considered applying this regulation to all businesses subject to the CCPA, as well as not requiring any type of reporting mechanism.

Reasoning: The Attorney General rejected these alternative approaches because they both fail to balance the public's interest in the effectiveness of the law with the burden such training and record-keeping obligations may pose on businesses, particularly small businesses. In reaching this determination, the Attorney General discussed with medium-sized and small business owners how they currently provide customer service and training procedures to employees, as well as how they meet other regulatory compliance mandates. Based on these discussions and internal analysis, the Attorney General took a hybrid approach, limiting the more rigorous training and record-keeping requirements to businesses that handle the personal information of approximately 10% of California's population.

F. Section 999.323, subdivision (a) – Method for Verifying Consumers

Alternative: The Attorney General considered and rejected an alternative approach of prescribing a specific method for all businesses to follow to verify the identities of persons submitting requests to know or delete personal information.

Reasoning: Given the wide variety of different industries subject to the CCPA, prescribing a particular method of verification may not provide the flexibility necessary to address all the different circumstances in which businesses and consumers interact, nor would it address changing data security standards and evolving technologies. Accordingly, businesses are held to certain guidelines that place the onus on businesses to determine the verification method that best fits their operations and protects consumers' personal information from unauthorized access. Because the CCPA holds businesses accountable for reasonable data security practices, businesses have the incentive to choose the most effective method for verification.

G. No Safe Harbor for GDPR Compliance

Alternative: The Attorney General considered and rejected the creation of a safe harbor exemption from the CCPA for businesses that are already complying with the European privacy law, known as GDPR (General Data Protection Regulation).

Reasoning: The Attorney General rejected this alternative because CCPA and GDPR have different requirements, different definitions, and different scopes. For example, GDPR prohibits collection without express consent; CCPA does not prohibit collection. GDPR does not have a right to opt-out of sale; the right to opt-out is a core right of CCPA. GDPR applies to both public and private sector entities; CCPA only applies to specific types of business. Because of this incompatibility, the Attorney General determined that a safe harbor would not effectively further the purposes of the CCPA. Further, both laws are relatively new, and thus, carving out a safe harbor so early in their existence appears premature.

H. No Revisions to Definition of Personal Information or Unique Identifiers

Alternative: The Attorney General considered and rejected alternatives to the definition of “personal information” or “unique identifiers” provided for in Civil Code section 1798.185, subdivisions (a)(1) and (a)(2).

Reasoning: Civil Code section 1798.185, subdivision (a)(1) and (a)(2), provide that the Attorney General shall adopt regulations that modify the definitions of personal information and unique identifiers “as needed” in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns. The Attorney General proposes these regulations in close proximity to the passage of the CCPA; thus, there are no intervening technological changes or data collection practices that would warrant the updating of these definitions. Similarly, businesses are still in the process of implementing the CCPA and these regulations, and thus, an updating of the definitions at this stage appears premature.

VIII. REGULATIONS MANDATED BY FEDERAL LAW

The proposed regulatory action does not contain any regulations that are identical to or conflicts with any corresponding federal regulation.

All initial statement of reasons requirements for the proposed regulations has been satisfied.

SF2018200870
53741451_2.DOCX

APPENDIX A

(Standardized Regulatory Impact Analysis)



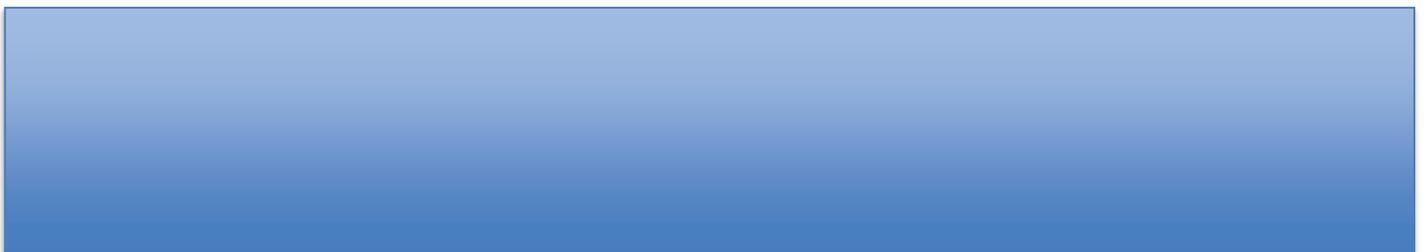
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL

Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations

**Prepared for: Attorney General's Office
California Department of Justice**

Prepared by: Berkeley Economic Advising and Research, LLC

August 2019



California Department of Justice

Primary Author(s):

David Roland-Holst
Samuel Evans
Drew Behnke
Samuel Neal
Liam Frölund
Yao Xiao

Berkeley Economic Advising and Research

1442A Walnut St. Suite 108
Berkeley, CA 94709
Phone: 510-220-4567
www.bearecon.com

Contract Number: 18-255U

Prepared for:

Attorney General's Office

Stacey D. Schesser

**Supervising Deputy Attorney General
Consumer Law Section - Privacy Unit**

David Roland-Holst
Project Manager

DISCLAIMER

This report was prepared as the result of work sponsored by the California Department of Justice (DOJ). It does not necessarily represent the views of the DOJ, its employees, or the State of California. The DOJ, the State of California, its employees, contractors, and subcontractors make no warrant, express or implied, and assume no legal liability for the information in this report; nor does any party represent that the uses of this information will not infringe upon privately owned rights. This report has not been approved or disapproved by the California Department of Justice passed upon the accuracy or adequacy of the information in this report.

Contents

Contents.....	3
1 Introduction	6
1.1 Background and Summary of Proposed Regulations.....	7
1.2 Major Regulation Determination	8
1.3 Public Outreach and Input	8
1.4 Regulatory Baseline.....	9
1.4.1 Baseline Costs to Businesses.....	10
1.4.2 Precedence from European Standards.....	12
1.4.3 Baseline Benefits to Consumers	12
1.4.4 Equity considerations.....	15
1.5 Incremental Impacts of the Proposed Regulation	16
1.5.1 Article 2: Notices to Consumers	16
1.5.2 Article 3: Business Practices for Handling Consumer Requests	17
1.5.3 Article 4: Verification of Requests	17
1.5.4 Article 5: Special Rules Regarding Minors	18
1.5.5 Article 6: Non-Discrimination	18
2 Impacts on California Businesses.....	20
2.1 How many firms are impacted by CCPA?.....	20
2.2 Article 3 Costs – Business Practices for Handling Consumer Requests	24
2.2.1 Operations and Technology Costs	24
2.2.2 90-Day Lookback Costs	25
2.2.3 Training Requirements.....	26
2.2.4 Record-Keeping Requirements	27
2.3 Article 4 Costs – Verification of Requests	27
2.4 Article 6 Costs – Non-Discrimination	28
2.5 Total Enterprise Compliance Costs	28
2.6 Incentives for Innovation	30
2.7 Small Business Impacts	31
2.8 Competitive Advantage/Disadvantages for California Businesses	31
3 Impacts on California Consumers	33
3.1 How many consumers are impacted by the CCPA?.....	33

3.2	Article 2 Benefits – Notice to Consumers	33
3.3	Article 3 Benefits – Business Practices for Handling Consumer Requests.....	33
3.3.1	90-day Lookback Requirement	33
3.3.2	Training Requirements.....	34
3.3.3	Record Keeping	34
3.4	Article 4 Benefits – Verification of Requests.....	34
3.5	Article 5 Benefits – Special Rules Regarding Minors.....	34
3.6	Article 6 Benefits – Non-Discrimination	35
4	Macroeconomic Impacts	36
4.1	Methodology	36
4.2	Scenarios	36
4.3	Inputs to the Assessment.....	37
4.4	Results	38
5	Fiscal Impacts	41
6	Economic Impacts of the Regulatory Alternatives	42
6.1	More Stringent Regulatory Alternative.....	42
6.2	Less Stringent Regulatory Alternative.....	42
6.3	Macroeconomic Impacts.....	43
7	Summary of Economic Results.....	45
8	References	46

Abbreviations

AB – Assembly Bill

AG – Attorney General of California

BEAR - Berkeley Economic Advising and Research

CCPA – California Consumer Privacy Act

CGE – Computable General Equilibrium

DOF – California Department of Finance

DOJ – California Department of Justice

FY – Fiscal Year

GDPR - General Data Protection Regulation

PI – Personal Information

SRIA – Standardized Regulatory Impact Assessment

1 Introduction

California is the fifth-largest economy in the world, with a sizeable market leading the development of new technologies. The state is also home to many businesses that have capitalized on the collection of private data from consumers. With the sophistication and scope of technology and data increasing daily, so has the extensive and intensive collection of consumer information by businesses. Neither state nor federal law have kept pace with these developments in ways that enable consumers to exert control over the collection, use, and protection of their personal information (PI). Survey research from the Pew Research Center demonstrates that consumers do not trust that their personal data is secure and would like to be in control of what information is available and who has access to it. For example, a 2015 survey found that only 7% of respondents were confident that their records would remain private and 90% of respondents would like to be in control of what personal data is available (Madden & Rainie 2015). Consumers are also unaware of how and what data is being collected about them when they use the internet, their smart phones, or other interactive devices. They are wary about how their data is used and sold to third parties, often without their knowledge or control, as well as lack of transparency, compounded by confusing terms of service that govern everyday online services, including social media platforms, e-commerce sites, and internet search engines.

Despite these concerns, the vast majority of consumers continue to use free services, which rely upon and monetize consumer personal information. This situation appears to be the result of a lack of understanding over how to control data collection, i.e. the majority of internet users (62%) do not know how to limit information that is collected about them by a website (Purcell 2012). Not only do many consumers lack the technical ability to protect their data, but the market power of many internet companies and interactions between others leave consumers few options to surrendering their privacy. This “privacy market failure” supports a general case for intervention in the public interest, a primary impetus for legislation such as the groundbreaking California Consumer Privacy Act (CCPA). As part of the CCPA, the California legislature tasked the Attorney General’s office with adopting regulations to implement many elements of the statute. This Standardized Regulatory Impact Assessment (SRIA) evaluates the impacts of these proposed regulations on the California economy.

1.1 Background and Summary of Proposed Regulations

The CCPA arose from a consumer-led, statewide ballot initiative that was headed for the November 2018 election. The goal was to empower consumers with the ability to learn what data businesses were collecting on them and vest them with the ability to stop the sale of their personal information. Before reaching the ballot however, the California legislature offered AB 375 in exchange for the withdrawal of the ballot measure. On June 28, 2018, AB 375 passed unanimously and was signed into law. The law offers the following privacy protections to consumers:

- **Right to Know:** Grants consumers the right to be informed about a business's practices regarding the collection, use, disclosure, and sale of PI, and also to be informed, in response to a verifiable consumer request, of the specific pieces of their PI held by the business.
- **Right to Delete:** Grants consumers to the right to request that a business delete any PI that the business has collected from the consumer, as well as direct any service providers to delete the PI, unless excepted.
- **Right to Opt-Out:** Grants consumers the right to direct a business that sells a consumer's PI to no longer sell their PI. For minors between the ages of 13 – 16, a business may not sell their personal information without affirmative authorization. For consumers under 13, the affirmative authorization to sell must be granted by the parent or legal guardian.
- **Right to Non-Discrimination:** A business cannot discriminate against the consumer for exercising any of the above rights. This includes denying goods or services, charging different prices, or providing a different level or quality of service. However, a business is able to offer a consumer's different rates (or service) if that difference is reasonably related to the value of the consumer's data.

The CCPA applies to all businesses in California that meet one or more of the following three thresholds: (1) has annual gross revenues in excess of twenty-five million dollars (\$25,000,000). (2) buys, sells, or shares the personal information of 50,000 or more consumers, households, or devices. (3) derives 50% or more of its annual revenue from selling consumers' PI.

The CCPA tasks the Attorney General with both exclusive enforcement of the law and rulemaking authority in furtherance of the CCPA. With respect to regulations, the law sets forth areas that require immediate rulemaking by July 1, 2020 (See Civil Code, § 1798.185, subd. (a)), and provides for ongoing, future rulemaking authority "as necessary

to further the purposes of this title” (id. at subd. (b)). Thus, the Legislature may have intended for rulemaking to commence on the specific, outlined areas in section 1798.185(a) so that the CCPA would be workable for businesses and consumers alike. In undertaking the preliminary rulemaking activities as required by the CCPA and the Administrative Procedure Act, the Attorney General solicited broad public participation at seven statewide forums and highlighted the list of areas in section 1798.185(a) for public comment. For this first-round of rulemaking, forthcoming regulations will address these priority areas, including how businesses shall respond and handle consumer requests, how consumers may submit verifiable consumer requests, and how businesses may offer financial incentives without discriminating against consumers who exercise their rights under CCPA. Future rulemaking may address any areas that require additional guidance.

As enacted, the CCPA mandates new obligations on businesses that would apply even without the force of the Attorney General’s regulations. For example, businesses would have to update privacy policies and develop a mechanism for providing notice to consumers at or before the point of collection. Some businesses may already have these mechanisms in place in light of other existing legal frameworks, including federal and international privacy laws. Businesses must also comply with the newest right afforded to consumers—the right to opt-out of the sale of PI—as these requests do not mandate any verification by the business. Thus, while the Attorney General’s forthcoming regulations will provide clarity on the operability of some of CCPA’s provisions, businesses will be subject to and must comply with many requirements of the law when it goes into effect on January 1, 2020.

1.2 Major Regulation Determination

A proposed regulation is determined to be a major regulation if the estimated economic impact of the regulation is expected to exceed \$50 million per year once fully implemented. Both the direct compliance costs and direct benefit of the proposed regulation are independently expected to exceed this threshold. Our preliminary estimate of direct compliance costs is estimated to be \$467-\$16,454 million over the next decade (2020-30), depending on the number of California businesses coming into compliance (details below). Therefore, DOJ implementation of CCPA qualifies as a major regulation, requiring a complete SRIA.

1.3 Public Outreach and Input

DOJ held seven public forums statewide to solicit broad public participation as part of its preliminary rulemaking activities for CCPA. DOJ also set up a dedicated portion of its website to keep the public informed of various CCPA rulemaking activities, including the

transcripts from each of the public forums. In total, DOJ received input from over 110 speakers at the public forums and over 300 written comments, which were also posted on DOJ's CCPA website.

1.4 Regulatory Baseline

The CCPA will result in both benefits to consumers and costs to businesses, but for the purposes of this SRIA, we are tasked with identifying the additional costs and benefits from the regulations needed to successfully implement the law. An assessment of the economic impacts of the proposed regulations requires identifying the incremental impacts of the regulation beyond what would have happened in the absence of the regulation. This counterfactual, the absence of the regulation, is referred to as the regulatory baseline and is developed in detail in this section.

As noted in the introduction, while the CCPA gives the California DOJ broad authority to write implementing regulations, many of the benefits and costs are likely to be incurred regardless of the specific regulations. Some of these economic impacts, whether compliance costs to businesses or benefits to California consumers, are part of the regulatory baseline and not directly attributable to the proposed regulations. This interpretation is supported by evidence showing that businesses are making large up-front investments in CCPA compliance strategies, based on their review of the statutory text, ahead of the issuance of the first round of regulations.¹ For consumers, the law, not the regulations, establishes the main privacy rights and benefits, which are therefore also assumed to largely be a part of the regulatory baseline.

The incremental regulatory impacts, for which we analyze the economic impacts in this SRIA, include regulatory actions proposed by DOJ that differ from how a regulated business might interpret the CCPA in the absence of guiding regulations. In other words, we assume that in the regulatory baseline, businesses either follow exactly what the CCPA requires or utilize full discretion in areas where the CCPA does not provide explicit guidance. In areas where this distinction is not clear, we default to assuming that the economic impacts are fully attributable to the regulation. We also include a detailed discussion of the baseline costs and benefits that we assume to be attributable to the CCPA. The intent of this is to highlight the potential costs attributable to the CCPA along with the potential incremental costs directly attributable to DOJ's regulations.

¹ The 2019 analysis, published by TrustArc Inc, found that 84% of respondents had started CCPA compliance efforts and 56% had begun implementing their CCPA compliance plans.

1.4.1 Baseline Costs to Businesses

The California Consumer Privacy Act of 2018 requires qualifying businesses operating in California to take a number of compliance actions that go beyond standard business practices prior to passage of the privacy law. New systems must be put into place to respond to requests from consumers exercising their rights under the law. In general, compliance costs associated with the CCPA fall into four categories:

1. **Legal:** Costs associated with interpreting the law so that operational and technical plans can be made within a business.
2. **Operational:** Costs associated with establishing the non-technical infrastructure to comply with the law's requirements.
3. **Technical:** Costs associated with establishing technologies necessary to respond to consumer requests and other aspects of the law.
4. **Business:** Costs associated with other business decisions that will result from the law, such as renegotiating service provider contracts and changing business models to change the way personal information is handled or sold.

Total CCPA compliance costs are likely to vary considerably based on the type of company, the maturity of the businesses current privacy compliance system, the number of California consumers they provide goods and services to, and how personal information is currently used in the business. A recent survey by TrustArc of businesses expecting to need to undertake compliance actions for CCPA found that 29% of businesses expect to spend less than \$100,000 (or nothing) on compliance, 32% expect to spend \$100,000-\$500,000, 20% expect to spend \$500,000-\$1,000,000, 15% expect to spend \$1,000,000-\$5,000,000, and 4% of businesses expect to spend more than \$5,000,000. While these estimates of costs are quite large, the majority of these economic costs are attributable to the CCPA, not the DOJ's regulations. Furthermore, the survey was only sent to businesses with more than 500 employees. Nearly 99% of California businesses have fewer than 500 employees.

The first cost category for CCPA compliance includes all legal fees incurred in preparing for the law. These costs can be quite large, ranging from \$50,000 to \$1,000,000, according to informal consultations. However, we assume that these costs are not attributable to the regulation, since businesses would need this legal advice regardless of the regulatory actions taken by DOJ.

Operational costs, which can include substantial labor costs as multiple departments in an organization coordinate a business' compliance strategy and workflow, are also almost

entirely attributable to the law. The CCPA is very clear about what rights consumers have and that businesses must respond to opt-out, deletion, and access requests. The majority of these costs, which are incurred even before the regulations are drafted, would be incurred regardless of how DOJ crafted the specific regulations. However, the operational compliance costs of the ongoing training requirements and some record-keeping requirements for firms with more than 4 million California consumers are directly attributable to the regulations and are therefore calculated in this assessment.

Technology costs, which cover the websites, forms, and other systems necessary to fulfill the CCPA compliance obligations, are also quite substantial due to passage of the CCPA. However, like operational costs, these are mostly attributable to the law, not the regulation. As an example, consider the “Do Not Sell My Personal Information” link required by the law. All CCPA-compliant companies must include this link on their webpages; however, the DOJ regulations will give them guidance on what must be included on the webpage to which the link directs consumers. While there might be some design costs that could be attributed to DOJ’s requirements, the vast majority of the cost of including the link is attributable to that requirement in the law.

For the areas of incremental economic impact that we have described above, the SRIA calculates, to the extent possible, an estimate of this cost for California businesses. To reiterate, these are the costs that we assume are directly attributable to DOJ’s regulations, not the CCPA overall.

To put these incremental costs in perspective, we generate a back of the envelope cost of CCPA compliance, including both the statute’s baseline costs and the incremental costs attributable to the regulations, using estimates from the TrustArc survey cited above. Assume that smaller firms (<20 employees) will incur \$50,000 in initial costs (the median of the lowest cost category)², medium-sized firms (20-100 employees) incur an initial cost of \$100,000 (the maximum of the lowest cost category in the survey), medium/large firms (100-500 employees) incur an initial cost of \$450,000, and firms with greater than 500 employees incur, on average an initial cost of \$2 million. Also assume that 75% of all California businesses will be required to comply with the CCPA (see Section 2.1 for detailed estimates of the number of firms affected by firm size and industry). The total cost of initial compliance with the CCPA, which constitutes the vast majority of compliance efforts, is approximately \$55 billion. This is equivalent to approximately 1.8% of California Gross State Product in 2018.

² The TrustArc survey only sampled privacy professionals from firms with at least 500 employees. Therefore, it is very possible that we are overestimating the compliance costs for smaller firms. However, in the absence of reliable compliance cost information for this category of businesses, applying the TrustArc estimates provides an upper bound on the total compliance costs.

1.4.2 Precedence from European Standards

The most comparable existing privacy regulation enacted is the European Union’s General Data Protection Regulation (GDPR). While the CCPA is narrower in scope – it only applies to California businesses meeting specific criteria (described in Section 2.1) whereas the GDPR applies to all businesses that process data of EU citizens – both regulations are designed to improve protections on consumers’ personal information and alter the way that personal data is collected and sold. In fact, standards and compliance for the GDPR have already imposed costs on many firms that operate in California. This reduces their expected cost of CCPA compliance and may offer useful guidance regarding the costs of enterprise adaptation to California standards. The EU’s impact assessment of the GDPR estimated average incremental compliance costs of approximately 5,700 Euros per year (European Commission 2012, Annex 9). This is consistent with other compliance cost estimates ranging from 3,000 to 7,200 Euros per year (Christensen et al 2013). Collectively, these costs represent a 16-40% increase in annual IT budgets (Christensen et al 2013). In addition to compliance costs, there is also evidence that the GDPR’s stricter data policies have reduced firm productivity in sectors that rely heavily on data (Ferracane et al 2019) with the biggest impacts found in firms devoted to data profiling (Cave et al 2012).

The GDPR also applies to many companies in California and, according to a recent survey by TrustArc, 83% of companies that have GDPR compliance requirements are expected to leverage some of their compliance programs for CCPA. For these companies, the work done on GDPR compliance will lower the compliance cost of CCPA, however given that the two privacy laws are not identical, businesses will not likely be able to fully apply their GDPR compliance systems to California consumers.

1.4.3 Baseline Benefits to Consumers

The CCPA’s benefits to consumers derive from the privacy protections granted by the law. These protections, described in the previous section, give consumers the right to assert control over the use of their personal information. The economic value to consumers of these protections can be measured as the total value of consumers’ personal information, which they can choose to prevent the sale of or even delete. Although the subjective value of this information to consumers is generally agreed to be great, it is extremely difficult to quantify the precise value of consumers’ personal information in the marketplace and estimates can vary substantially. There is, for example, no universal method for pricing personal information. It is frequently argued that the value of personal information faces too many barriers to be accurately priced. Either data is dependent on trade secrets and algorithms, is too context-specific, or the underlying value, such as privacy, is intangible. Indeed, even companies who use

personal information as primary strategic asset typically have difficulty assigning value (Short and Todd 2017). That being said, assigning value to personal data is not impossible. Although there is not a single universal value, there are several approaches that have been used to price information.

One approach to estimating the value of consumers' personal information is to carry out experiments where participants are given options to pay different prices for different levels of privacy protections. Using this approach, one experiment found that consumers assigned \$1.19-\$4.05 of value per app to personal information collected by smartphone apps (Savage and Waldman 2017). Scaling this up to the approximate number of apps downloaded by Californians in 2017³ suggests the aggregate value of consumers' private information on the app marketplace to be \$1.6 – 5.4B.

An alternative approach to measuring the value of CCPA's protections of personal information is to estimate the price businesses are willing to pay for it. Several efforts have been undertaken to collect and publish the price that data brokers charge for a typical consumer's data. For example, *The Financial Times* collected data on prices companies pay for different types of basic personal information (age, gender, marital status, etc.). Using this data, they published a calculator that allows individuals to estimate the value of a one-time sale of their basic personal data.⁴ General information about a person such as their age and gender were found to be worth \$0.0005 per person. However, milestones in peoples' lives such as marriage, buying a car, getting divorced, etc. were worth more. The price of information that a woman is pregnant, for example, was priced at \$0.11 per person. Collectively, the total value of the 61 basic information items examined sums up to approximately \$4.83 for the average person. Other analogous efforts have examined more detailed private data, including financial history, and estimated a value of \$277.65 per person for the one-time sale of these pieces of personal information.⁵ These estimates can be used to calculate the aggregate value of consumers' personal information. There are approximately 35M internet users in California,⁶ therefore using the Financial Times estimates the implied total value of consumers' basic information under protection would be approximately \$169M while the implied total of consumers' more sensitive personal information according to the SWIPE tool would be \$9.7B. These numbers illustrate that while, on an individual level, most personal information is at most moderately valuable, the aggregate value to consumers

³ Americans had approximately 11.3B app downloads in 2017 [www.statista.com/statistics/249264/countries-ranked-by-number-of-app-downloads/]. Given Californians are 12% of the U.S. population, and assuming Californians download apps at the same rate as other Americans, these numbers suggest Californians downloaded approximately 1.1B apps in 2017.

⁴ <https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2z2agBB6R>; Steele et al 2013.

⁵ http://turbulence.org/Works/swipe/swipe_data_cal.html

⁶ Census 2015 Supplementary Survey/American Community Survey (C2SS/ACS) (U.S. Census Bureau, 2010).

is large. Given the thousands of pieces of personal information collected by businesses, it is not realistic for these estimates to be comprehensive of all personal information. Instead, these estimates can be viewed as lower bound estimates on the value of basic, and more detailed, personal information that indicate the magnitude of the value of consumer data that the CCPA covers.

A final approach estimates the value of personal data based on financial records on a per-user or per-record basis. Common financial records include market capitalization, revenue, or net income. Revenue, and especially advertising revenue, is the most robust indicator as it reflects the market value for access to personal data. While finding the average revenue per user (ARPU) is relatively straightforward, decisions must be made about what firms to include. Typically, large tech companies that derive the majority of their revenue from personal data are used to price the value of personal data. However, the per-company approach is piecemeal and although large tech companies represent the majority of advertising revenue, they do not capture all of it. We therefore instead choose to focus on total digital advertising revenue, which is reported annually by the Interactive Advertising Bureau (IAB) trade-group. This measure reports all internet/mobile/online advertising revenue in the United States. Unlike traditional advertising, where all customers receive the same ad, online advertising is defined by its use of targeted (i.e. personal) ads. Therefore, this measure arguably captures the market value of personal data in the United States.

The IAB reports total advertising revenue split between desktop and mobile. Each of these categories are further subdivided between an additional four categories: Search, Banner, Video, Other. Of these categories, we assume search, banner, and video advertising all rely on personal data to target ads. The other category is comprised of classifieds, lead generation, and audio (podcasts), whose use of personal data is less clear. With estimates for total online advertising revenue for search, banner, and video the challenge becomes matching these estimates to the number of desktop and mobile phone users in the United States. Using ACS data, we are able to find the total number of internet users with both a computer and mobile, or only mobile, or only computer. With these estimates we are then able to estimate that ARPU for Mobile and Desktop online advertising. To reach estimates for the total value of personal data for California consumers we then take the ARPU estimates and multiply by the relevant number of computer and/or mobile users in California.

We find that the 2018 ARPU for search, banner, and video adds are \$135.71 (desktop) and \$266 (mobile). With an estimated 30.9 million desktop users and 31.7 million mobile users in California this represents a total value of \$4.2 billion and \$8.4 billion respectively.

Overall, this would suggest that value of personal information used for advertising in California is over \$12 billion annually.

The above estimates suggest that the aggregate value of personal data that falls under the CCPA is large, likely on the order of magnitude of tens of billions of dollars. Each of these effects should be considered cumulatively as well. The value of personal information based on data brokers is separate from that of digital advertising. Therefore, combining those estimates suggests the total value of personal data would exceed \$20 billion annually. Furthermore, since personal data is non-rival, the sale of one personal data profile does not preclude the sale of an additional one. This means that not only can specific data brokers sell the same profile numerous times, but that different companies can sell a profile representing the same individual as well. Thus, these above estimates represent a lower bound and should be taken as conservative values for personal information.

That being said, consumers only receive maximal benefits if they choose to exercise the privacy rights given to them and not everyone is likely to do so, although, available evidence indicates that a substantial portion of consumers have preferences that align with exercising rights provided by the CCPA. In a 2012 survey from the Pew Research Center, roughly two-thirds of consumers (68%) reported that they did not like targeted advertising because they did not want to have their online behavior tracked and analyzed (Purcell 2012). Moreover, a 2015 Pew survey found that 90% of respondents preferred to be in control of what personal information is available and being utilized by businesses (Madden & Rainie 2015). The CCPA provides consumers the opportunities to exercise these preferences by becoming informed of how their personal information is being collected and used, limiting the sale of this information, and requesting that it be deleted.

1.4.4 Equity considerations

The CCPA will introduce differential benefits for consumers largely related to wealth and income. While the CCPA increases the ease with which consumers can access, control, delete, and stop the sale of their data, some users may be unable to navigate the procedures required to access these rights. The CCPA requires that businesses make it straightforward for an average consumer to exercise their privacy rights. However, there is no guarantee that all consumers will be able to understand how to manage these processes. Insofar as other personal characteristics correlate with computer literacy, there may be equity concerns whether disadvantaged groups disproportionately do not exercise the privacy rights afforded to them by the CCPA. Furthermore, the stipulation that businesses can charge consumers for their services means that low-income groups may be more likely to give up their personal information in exchange for services while high-income groups are more likely to pay the service fee to protect their data.

Furthermore, there are serious equity considerations related to the ability for consumers to pay for a digital service using either money or data. When paying with data, users consent to allow businesses to use their data in return for services. Conversely, the payment option would allow users to make some type of monetary payment (either one-off or monthly) to use a service and explicitly forbid businesses to use their data. This suggests that low-income groups may be more likely to give up their personal information in exchange for services while high-income groups will pay the service fee to protect their data. In turn, the CCPA could create a system of two-tiers, where higher socio-economic groups are able to protect their personal information and disadvantaged groups have no choice but to allow their data to be used.

1.5 Incremental Impacts of the Proposed Regulation

In this section we identify provisions in the proposed regulation that are assumed to have incremental economic impacts that deviate from the regulatory baseline. For each article in the proposed regulation, we briefly describe the general purpose of the article and in instances where no incremental impact is assumed, we provide a justification for this assumption.

1.5.1 Article 2: Notices to Consumers

This section of the proposed regulation establishes rules regarding how businesses must notify consumers about their rights under the CCPA. There are four general notification requirement regulations developed by DOJ:

1. **Notice at Collection of Personal Information** - The regulations detail requirements for businesses to provide a notice communicating to consumers what type of information is being collected and for what purpose.
2. **Notice of the Right to Opt-Out of the Sale of Personal Information** - The regulations detail notification requirements for businesses that sell consumers' personal information and provide guidance on how businesses must communicate to consumers that they can opt out of the sale of their information to third parties.
3. **Notice of Financial Incentive** - The regulations detail notification requirements for businesses to clearly notify the consumer of financial incentives or price differentials being offered in exchange for using (internally or through sale) the consumer's personal information.
4. **Privacy Policy** –The regulations detail requirements for businesses to disclose in a privacy policy their online and offline practices regarding the collection, use,

disclosure, and sale of personal information, and of the rights of consumers regarding their PI.

We assume that none of the economic impacts associated with these notification requirements are directly attributable to the proposed regulation. Because notification requirements are required under the CCPA, the economic impacts of developing these notifications are part of the regulatory baseline. The DOJ regulations provide guidance to businesses on how they must structure the notification requirements but the resources required to do this are not likely to be different than what businesses would otherwise do to meet CCPA requirements.

1.5.2 Article 3: Business Practices for Handling Consumer Requests

This section of the proposed regulation establishes rules about how businesses must respond to personal information requests from consumers.

Establishing processes to respond to consumer requests is likely to require businesses to incur substantial costs. Most of these costs are attributable to the CCPA and not to DOJ's implementing regulations; however, there are certain aspects in Article 3 of the proposed regulation where DOJ had considerable flexibility to exercise discretion in drafting the regulations and these areas are assumed to have economic impacts attributable to the regulations rather than the CCPA. The incremental impacts include costs and/or benefits associated with:

1. Additional technology and operational costs for establishing systems for businesses and service providers to respond to consumer requests.
2. Notification to third parties to whom personal information was sold within the past 90 days, if a consumer makes an opt-out request.
3. Training requirements for employees in businesses that handle the personal information of more than 4 million consumers.
4. Recording-keeping requirements for businesses that handle the personal information of more than 4 million consumers.

All other economic impacts associated with language in Article 3 are assumed to be attributable to the CCPA and are therefore included in the regulatory baseline.

1.5.3 Article 4: Verification of Requests

Article 4 of the proposed regulation establishes rules about how business must go about verifying the identity of consumers making personal information requests. This is an area

where the CCPA gives DOJ considerable discretion in crafting the regulations. DOJ has chosen to separate verification of consumer requests into two categories: verification of consumers who have a password-protected account with a business and consumers who do not have a password-protected account with a business.

For consumers that have a password-protected account with a business, if the business is following existing privacy laws then the password authentication process is likely sufficient for verifying a consumer's identity. In this case, we assume that the regulations will have little or no incremental economic impact for consumer verification.

However, for consumers who exchange personal information with a business but do not have a password-protected account, the business must verify the identity of the consumer to either a reasonable degree of certainty or a reasonably high degree of certainty depending on the nature of the request. This may require matching at least two data points provided by the consumer to information maintained by the business, or three pieces of PI provided by the consumer with information maintained by the business and a signed declaration under penalty of perjury. The economic impact associated with this verification process is assumed to be attributable to the regulation and thus is addressed in this analysis.

1.5.4 Article 5: Special Rules Regarding Minors

The CCPA specifies that if a business collects personal information from minors 16 years or younger, it must obtain the affirmative authorization of the minor (if 13-16 years of age), or their parent or guardian (if the minor is under 13 years of age), to sell that information. The DOJ regulations outlined in Article 5 specify the process for opting-in. DOJ's regulations are meant to allow businesses to build on existing processes and systems they use for verifying parental consent under the Children's Online Privacy Protection Act (COPPA). However, COPPA requires consent for collection of data, whereas the CCPA requires consent for sale. Therefore, the DOJ regulations will require that additional notification of consent for sale. Any impacts associated with this can be directly attributable to the regulations.

1.5.5 Article 6: Non-Discrimination

The non-discrimination regulations proposed by DOJ attempt to clarify language in the CCPA about business practices that treat consumers who exercise their rights under the CCPA differently, such as by providing financial incentives or differential services/prices. The CCPA's anti-discrimination clause says that businesses cannot discriminate against consumers for exercising their CCPA rights (opt-out, right to know, and right to delete); however, a business can offer a financial incentive or a price or service difference if it is reasonably related to the value of the consumer's data to the business. While these

provisions are included in the CCPA, and are therefore part of the regulatory baseline, the CCPA directs DOJ to provide guidance to businesses on exactly how a business should determine the value of a consumer’s data. We assume that there are economic impacts associated with how this definition of value is determined that are directly attributable to the DOJ regulations and thus should be included in the SRIA.

Table 1: Incremental Economic Impacts from DOJ’s CCPA Regulations

Section of the Regulation	Incremental Economic Impacts
Article 2: Notices to Consumers	None attributable to regulation
Article 3: Business Practices for Handling Consumer Requests	(1) Fraction of technology and operational costs of implementing systems for handling requests. (2) 90-day third-party notification of opt-out requests. (3) Training requirements (4) Record-keeping requirements
Article 4: Verification of Requests	(5) Cost of verifying identity for non-accountholders
Article 5: Special Rules Regarding Minors	(6) Additional notification and verification requirement beyond COPPA.
Article 6: Non-Discrimination	(7) Impact associated with how the value of personal information can be calculated by businesses.

2 Impacts on California Businesses

In terms of measurable direct costs, the most consequential aspect of CCPA will be investments in compliance activity by enterprises operating in California. This section describes the incremental compliance cost estimates used in this SRIA, representing each of several categories of incremental impact identified in the regulatory baseline.

2.1 How many firms are impacted by CCPA?

Not all businesses that handle the personal information of California residents are required to comply with the CCPA. The law established three thresholds, each of which would trigger compliance requirements if reached. They are:

1. A business has annual gross revenues of more than \$25 million,
2. A business buys, sells, or shares the personal information of more than 50,000 consumers, households, or devices per year,
3. A business derives 50% or more of its annual revenue from selling consumers' personal information.

As a lower-bound estimate of the number of businesses that will be required to comply with CCPA, we use 2017 Survey of U.S. Businesses (SUSB) data from the U.S. Census Bureau. This data reports the number of firms by sector and number of employees for California. Because the data does not include data on business revenue, we assume that the average employee generates approximately \$100,000 in annual revenue. Based on this assumption, firms with more than 250 employees will meet the \$25 million CCPA threshold. Employee size categories in the SUSB data are reported for businesses with 100-499 employees and businesses with 500 or more employees. We assume that all businesses with 500+ employees will be subject to the CCPA and 37.5% of businesses in the 100-499 employee category will need to comply with the law.

A lack of data prevents us from estimating with precision the number of businesses that meet the other threshold requirements in the CCPA. However, it is likely that the 50,000 PI requirement and the 50% annual revenue requirement will apply to many businesses with annual revenues less than \$25 million. For example, any firm that collects personal information from more than 137 consumers or devices a day will meet the 50,000 threshold. To provide an upper bound on the number of firms potentially affected by the CCPA regulations, we consider two alternative assumptions. We assume that either 50% or 75% of all California businesses that earn less than \$25 million in revenue will be covered under than CCPA. A survey completed by the International Association Privacy

Professionals (IAPP) found that 8 out of 10 surveyed businesses believed that they would need to take compliance actions as a result of the CCPA. Because the survey went only to businesses in certain sectors likely to be covered by the law, the 50-75% upper-bound compliance range is reasonably supported by empirical evidence.

The SRIA requires an analysis of the impact of proposed major regulations on California businesses. However, the CCPA will also affect businesses that provide goods and services to California consumers. There are likely to be many businesses that are not located in California (and therefore not captured in SUSB statistics) but serve California customers. The economic impact of the regulations on these businesses located outside of California is beyond the scope of the SRIA and therefore not estimated.

Table 2 shows the total number that would either exceed the \$25 million annual revenue threshold or require compliance under the 50% and 75% scenarios. While the law says that medical information is not covered as personal information under the CCPA, we assume that large firms in the health care sector will still likely need to comply with the law as they collect other non-medical personal information on consumers. We also show the number of firms with greater than 500 employees, which will be used for assessing certain compliance costs later in the analysis.

The lower bound estimate of the number of businesses affected by the proposed regulations is 15,643. The upper bound estimates, depending on whether one assumes 50% or 75% of businesses will be impacted, ranges from 383,323 to 570,066. This large range of potentially impacted businesses will have important implications for the total compliance costs of the proposed regulations.

The SRIA requires an analysis of the impact of proposed major regulations on California businesses. However, the CCPA will also affect businesses that provide goods and services to California consumers. There are likely to be many businesses that are not located in California (and therefore not captured in SUSB statistics) but serve California customers. The economic impact of the regulations on these businesses located outside of California is beyond the scope of the SRIA and therefore not estimated.

Table 2: Number of California Businesses Meeting the \$25 Million CCPA Revenue Threshold

NAICS Code	Description	>\$25 million revenue threshold	50% Threshold	75% Threshold	Firms with 500+ Employees
11					21
21				434	61
22	Utilities	46	285	408	40
23	Construction	573	35,592	53,256	264
31-33	Manufacturing	1,612	18,352	27,016	1,025
42	Wholesale Trade	1,657	26,134	38,658	1,087
44-45	Retail Trade	1,079	35,382	52,746	656
48-49	Transportation & Warehousing	832	10,154	14,923	615
51	Information	678	8,579	12,634	469
52	Finance and Insurance	818	14,843	21,962	606
53	Real Estate, Rental, Leasing	461	21,628	32,289	304
54	Professional, Scientific, and Technical Services	1,728	58,404	87,038	1,137
55	Management of Companies and Enterprises	1,537	2,196	2,708	1,171
56	Administrative/Support/Waste Mgmt. Svs.	1,120	19,100	28,290	722
61	Educational Services	411	6,386	9,479	202
62	Health Care and Social Assistance	1,165	46,078	68,842	550
71	Arts, Entertainment, and Recreation	281	11,806	17,634	151
72	Accommodation and Food Services	986	33,024	49,301	470
81	Other Services (except Public Administration)	550	34,133	51,046	307
99	Industries Not Classified	0	1,473	2,210	0
Total		15,643	383,328	570,066	9,858

2.2 Article 3 Costs – Business Practices for Handling Consumer Requests

There are four specific incremental costs for businesses complying with DOJ’s Article 3 regulations that are assumed to be directly attributable to the regulation. These are:

- a) The small fraction of technology and operations costs that will directly exceed an average businesses or service provider’s interpretation of the CCPA due to the specificity of the regulations.
- b) The costs of complying with DOJ’s 90-day lookback requirement for firms selling personal information to third parties.
- c) The more detailed training requirements for firms handling the personal information of more than 4 million California consumers.
- d) The more detailed record-keeping requirements for firms handling the personal information of more than 4 million California consumers.

2.2.1 Operations and Technology Costs

We assume that a small fraction of the operational and technology costs associated with the CCPA are likely to be attributable to the regulation. Operational costs are predominantly a one-time cost of establishing workflows, plans, and other inter-departmental non-technical systems to determine the business’ best compliance pathway under the CCPA. These costs are largely labor costs associated with meetings and compliance planning. For illustrative purposes we assume that for large companies, a separate employee from three different departments in an organization will need to coordinate with weekly meetings (2 hours each) for 6 months. For the value of these employees’ time, we assume the 2018 median annual salary of a data privacy officer (\$123,050). We assume that 10% of these costs are directly attributable to the regulation, with the rest attributable to the CCPA baseline. The total annual cost attributable to the regulation for a representative firm is therefore \$959 in the initial year of compliance. Applied to all firms with revenue greater than \$25 million per year, the total compliance costs for operational compliance is approximately \$15 million. Applying this incremental cost using the 50% and 75% thresholds increases the total operational costs attributable to the regulation to \$368 million and \$547 million.

Costs associated with developing technological systems to comply with the CCPA are also likely to be significant and will vary considerably by firm and sector. For large firms, many are likely to allocate in-house engineering resources to develop specialized systems. Firms that handle less personal information and that are not using that personal information as a key aspect of their business models are not likely to develop complicated

technological platforms to respond to CCPA requests, especially in the early phase of CCPA compliance. New technologies may develop over time to provide businesses with technological platforms that do provide these services. Because of considerable variation and uncertainty in technology costs prior to CCPA implementation, we assume that 25% of total expected compliance costs reported by firms are likely to be for the technology requirements necessary to respond to CCPA requests. Based on the TrustArc firm survey cited above, we assume a central value of for technology costs of \$75,000 per firm, 10% of which we assume is directly attributable to the DOJ regulations.

If a consumer contacts a service provider with a request to know or request to delete, according to the DOJ regulations, the service provider must provide the consumer with the contact information of the business on whose behalf the service provider processes the information when feasible. The CCPA requires that service providers comply with businesses' direction to delete/stop selling personal information but does not provide guidance on whether or how a service provider should respond directly to consumers. The regulatory requirement that service providers respond to consumer requests by providing the contact information for the primary PI-collecting business will likely require the service provider to build out a process for responding to requests and identifying which business it is servicing. It is not possible to quantify this cost ex ante since there are no data sources that identify the number of service providers located in California. However, we would expect it to be a small fraction of the costs incurred by businesses handling personal information directly from consumers as these companies build out the technology and operational systems necessary to respond to consumer requests.

2.2.2 90-Day Lookback Costs

The DOJ's CCPA regulations specify that if a consumer makes an opt-out of sale request, the business must notify any third party that was sold the consumer's information in the past 90 days that the consumer has withdrawn their consent to sell the data. These third parties are then no longer allowed to sell the data. The CCPA did not specify that the third party who had received the data up to 90 days prior must discontinue further sales of the data. The law could instead have been interpreted as saying that after an opt-out request is made, the firm could no longer make additional sales of the data, but that previous sales of personal information were not covered.

The incremental compliance cost associated with this regulation is the extra work required by businesses to notify third parties that further sale is not permissible. Reliable data was not available to quantify this impact, which would require knowing how many businesses sell personal information to third parties. However, businesses that do sell personal information will need to retain records to track these sales and must allocate resources to communicating with third parties once an opt-out request is made. For larger

companies, it is quite plausible that this notification process will be built into automated systems so that additional staff resources are not required. If this is the case, the incremental compliance cost will be cost associated with building this capacity into the data mapping strategy and back-end technologies.

2.2.3 Training Requirements

The CCPA requires that individuals within a business that handle consumer inquiries are aware of the provisions of the law. There is no detailed guidance stating how these individuals will be made aware of the law and a plausible interpretation by a business would be to assume that privacy professionals are aware without any formal training. Under such an interpretation, the regulatory baseline would have no costs associated with employee training.

The DOJ regulations specify that firms collecting, buying, selling, or sharing the personal information of more than 4 million California consumers (approximately 10% of the State's population) must "establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA." We assume that there are additional costs associated with this training policy that are directly attributable to the regulations.

For simplicity, we assume that all firms with more than 500 employees will fall under the training requirements. This assumption is purely speculative since there is no detailed data on how many California consumers all companies in the State have. Industries are likely to fall into this compliance category if they are located in California, have little competition for their goods or services in the State, and collect personal information. For example, large electric power utilities are likely to use personal information from many California consumers for business purposes. Technology and social media companies that have large-scale adoption of their services are also likely to fall into this category.

To calculate the cost of training, we assume that the training will consist of requiring data professionals to read prepared training documents on the CCPA law and regulations. We assume that for large firms, there will be a team of approximately 5 privacy professionals that may handle consumer requests or be responsible for the business's CCPA compliance. Each individual will require two hours to complete the training and that the cost to the business is the opportunity cost of these employees' time. Assuming an average wage of \$123,050 (\$61.50/hour), the total cost per business is assumed to be \$615/year ($\$61.5/\text{hr} \times 2 \text{ hours} \times 5 \text{ individuals}$). The total compliance cost for the 9,858 businesses with more than 500 employees is \$6.062 million per year.

2.2.4 Record-Keeping Requirements

Similar to the training requirements, the DOJ specifies additional record-keeping requirements for firms that collect, buy, sell, or share the personal information of more than 4 million California consumers. These businesses must compile a number metrics on consumer requests and business responses from the prior year. For example, the business must estimate the number of requests to know, requests to delete, and requests to opt out that were (1) received, (2) complied with, and (3) denied. The business must also compile the number of days that the business took to substantively responded to requests to know/delete/opt out.

For estimating the incremental cost of this recording-keeping requirement, we make several assumptions. First, because the businesses affected by this record-keeping requirement are already likely to have mature systems for identifying, processing, and analyzing personal information from their data mapping and consumer response systems, we assume that there is no incremental cost of actually collecting this information. We do assume that there is a labor cost associated with processing and reporting the information in a format in the businesses privacy policy that is in compliance with the DOJ regulations. We assume that this activity will take approximately two (2) days of time (16 hours) from a data privacy professional. Assuming a rate of \$61.5/hour, each firm will incur a labor cost of \$984/year. The total cost for businesses assumed to exceed the 4 million consumer threshold is \$9.7 million per year. This cost is likely to be ongoing since the metrics must be reported every year.

2.3 Article 4 Costs – Verification of Requests

As noted in the regulatory baseline, there may be some additional compliance costs attributable to the regulation from a business needing to confirm the identity of consumers without accounts making CCPA requests. In theory, the costs associated with this compliance action could be calculated as follows:

Cost per firm = Number of California Consumers Doing Business with the Firm
 x % of the Consumers Without an Account
 x % of Consumers Making a CCPA Request
 x Incremental Cost per Person of Verification

Each of these factors is likely to vary considerably from business to business and there are no data points that would allow an estimation of this impact ex ante. However, if businesses build out efficient systems for complying with other aspects of the CCPA related to handling consumer requests, the incremental cost of matching the identity of a consumer to personal information that the business already has is likely to be quite low. For companies that routinely handle personal information and have sophisticated privacy

systems in place, this verification process is likely to be automated. There will be an upfront cost of integrating this verification into the larger privacy ecosystem but marginal cost for an additional consumer verification could be close to zero. On the other end of the spectrum, for businesses that attempt to manually verify consumers without an account, the marginal cost would be the labor cost associated with having staff dedicated to this verification process. In this case, the cost would depend on the number of verification requests being made and the variable cost is likely to be quite high relative to any initial investments in developing the systems for automating verification.

2.4 Article 6 Costs – Non-Discrimination

The CCPA states that DOJ should adopt regulations regarding financial incentive offerings. The DOJ chose to outline eight broad methodological approaches that businesses could use to determine the value of consumer data for financial incentive offerings. For example, a business can use either the marginal or average value of a typical consumer's PI to the business. They can also base their determination of value on revenues, profits, or costs associated with the PI. As a final category, the regulations say that the business can use any other method of estimating the value, so long as it is made in good faith. Essentially, DOJ is telling businesses that they can use whatever method they prefer, so long as there is an actual method developed that is reasonable. The cost associated with this provision is simply the cost to develop the method for businesses that are using financial incentives. There is therefore an initial labor cost associated with developing and documenting the method. The various methods are likely to become standard business practice and therefore we assume that a business will likely need to devote about 1 day (8 hours) towards developing a methodological approach. Assuming an average hourly rate of \$61.50, the average cost for a typical business will be approximately \$492. Applied to the 15,646 businesses with revenue greater than \$25 million per year, the total cost would be \$7.7 million. Applied to the 383,382 and 570,066 businesses in the 50% and 75% compliance scenarios, costs associated with developing these methodologies would be \$188.6 million and \$280.5 million, respectively.

2.5 Total Enterprise Compliance Costs

Table 3 shows the total estimated costs by sector for the proposed regulations. Costs are estimated for each of the three thresholds used to assess the number of potentially affected firms. The most conservative estimate is for firms that exceed the \$25 million annual revenue threshold, while the 50% and 75% threshold reflect assumptions that many additional firms would be subject to DOJ's CCPA regulations. It is important to note

that these costs only reflect quantified compliance costs. Some compliance costs noted in the previous sections did not have enough empirical evidence to support a compliance cost estimate. Furthermore, the novel nature of the CCPA and uncertainty regarding the expected compliance actions by firms across a diverse set of sectors should cause the reader to interpret these compliance costs estimates with caution.

Table 3: Total Estimated Compliance Costs (million 2019\$)

NAICS Code	Description	>\$25 million revenue threshold	50% Threshold	75% Threshold
11				40.5
21	Mining, Quarrying, and Oil and Gas Extraction			12.6
22	Utilities	1.4	8.3	11.8
23	Construction	16.9	1,026.8	1,536.1
31-33	Manufacturing	48.1	530.8	780.7
42	Wholesale Trade	49.5	755.3	1,116.5
44-45	Retail Trade	32.2	1,021.3	1,522.0
48-49	Transportation & Warehousing	25.0	293.8	431.3
51	Information	20.3	248.1	365.1
52	Finance and Insurance	24.6	429.0	634.3
53	Real Estate, Rental, Leasing	13.8	624.2	931.6
54	Professional, Scientific, and Technical Services	51.6	1,686.0	2,511.6
55	Management of Companies and Enterprises	46.2	65.2	80.0
56	Administrative/Support/Waste Mgmt. Svs.	33.5	551.9	816.9
61	Educational Services	12.2	184.5	273.7
62	Health Care and Social Assistance	34.5	1,329.6	1,986.0
71	Arts, Entertainment, and Recreation	8.3	340.7	508.7
72	Accommodation and Food Services	29.2	953.0	1,422.4
81	Other Services (except Public Administration)	16.4	984.8	1,472.5
Total		466.9	11,069.4	16,454.2

2.6 Incentives for Innovation

The CCPA will generate incentives for innovation across a range of new privacy products and services for consumers. Firms have already begun announcing new features intended to assist consumers with managing their private data while using the firm's products. These types of innovations are likely to accelerate. In addition to product specific features, there will also be incentives for provision of new services assisting consumers with utilizing CCPA protections to monitor and manage their data across products. Because consumers are required to communicate with each business individually, there is potential demand for a service that allows consumers to manage these many requests through a single interface and advises consumers on how best to utilize their rights to privacy overall.

Like consumers, firms will also demand new products and services in relation to the CCPA. New businesses or services are likely to be developed in order to assist firms with CCPA compliance. While initial efforts may focus on helping individual firm compliance, there will likely eventually be a relatively cheap standardized compliance assistance product developed analogous to software services designed to help individuals fill out their tax returns. Because of the large number and wide range of firms affected by the CCPA, there will be strong incentives to offer a relatively inexpensive product that can be marketed to a wide variety of firms, including smaller businesses, that do not have the internal capacity to manage compliance.

The CCPA will fundamentally change how firms work with personal data. Some industries will be forced to completely revise their business models to incorporate the newly required data protections. Data brokers, for example, will need to fundamentally change the way they operate. Adapting to the new privacy conditions will require innovations in the way firms use data. New data management systems that ensure privacy standards will need to be developed along with new techniques to extract useful information from data with obscured identifying personal information. The CCPA may, somewhat counterintuitively, also provide firms with new opportunities to expand data-based research and products. If the CCPA increases consumers' trust of data protections it could actually *increase* the amount of data that consumers are willing to share with firms. Despite the additional controls put on data use, increased access to users' data could help improve business' capacity to produce and bring research to market as well as increase firm capacity for product innovation.

2.7 Small Business Impacts

Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises. Conventional wisdom may suggest that stronger privacy regulations will adversely impact large technology firms that derive the majority of their revenue from personal data, however evidence from the EU suggests the opposite may be true. Over a year after the introduction of the GDPR, concerns regarding its impact on larger firms appear to have been overstated, while many smaller firms have struggled to meet compliance costs. Resources explain this dichotomy as large technology companies are often several steps ahead of both competitors and regulators. In fact, some have even argued that the GDPR has provided a competitive advantage to large firms as their significant in-house regulatory resources have allowed them to adjust quicker, while smaller competitors have struggled to adapt (Scott et al. 2019).

Small firms in California will face similar pressures. Large technology firms that are already GDPR-compliant will likely find it easier to become CCPA-compliant. Furthermore, with more revenue, large companies are better suited to absorb up-front compliance costs. Another significant risk to small businesses is uncertainty. Even after the roll out of regulations, interpretation and implementation present additional challenges to ensure full compliance for small enterprises. In the example of the GDPR, some firms report struggling with understanding compliance requirements, which has made compliance harder for small firms (Scott et al 2019).

These concerns will present real challenges for small businesses in the short term. In the long term however, the differential impacts will be smaller as third-party service providers enter the market to offer small businesses low-cost tailored compliance solutions. Although some small businesses will use in-house resources to become compliant, we expect that many others will outsource this work to dedicated firms. As competition in this new market increases, we expect overall costs to fall, limiting the differential impacts between small and large businesses in the long run.

2.8 Competitive Advantage/Disadvantages for California Businesses

For firms that operate within the state of California, the regulation will provide a competitive disadvantage relative to firms that operate only outside of the state. This is purely a reflection of compliance costs as firms that are subject to the regulation will face higher costs than those that are not. The most affected firms are those that have over \$25 million in revenue that have competitors of a similar size operating only outside of California. These firms will be at a disadvantage when competing in markets outside of California, as they will be faced with higher compliance costs relative to their competitors.

We anticipate the competitive disadvantage to be small, however. Given the size of the California economy, previous legislation that was unique to California has in turn set national standards as firms find it easier to adopt California's requirements to all products and services rather than provide differentiated services. Furthermore, there is likely limited direct competition between firms that would be subject to the regulation and those that would not. Either the firm is small and localized and would not compete directly with outside firms or is large enough that outside competitors have a California component to their business already and would be subject to the regulation as well.

On the other hand, the regulation may also provide a future competitive advantage for affected firms that are required to come into CCPA compliance now by creating additional barriers to entry for future competitors considering entering into the California market. Moreover, if the CCPA is a precursor for future privacy regulations at the additional state or federal level, then firms already in compliance with the CCPA will have a competitive advantage over firms that are not. Indeed, this already appears to be the case as legislators in nine states have introduced bills that would follow either all or part of the model established in the CCPA. Therefore, firms that become CCPA-compliant now will be better positioned to adapt to future privacy protection regulations.

3 Impacts on California Consumers

As its name implies, the primary impetus for CCPA is to improve the wellbeing of California consumers. While much of the policy dialog on individual privacy emphasizes non-pecuniary benefits, this economic assessment confines itself to measurable economic benefits that could reasonably be expected to accrue to private individuals from CCPA implementation. This section discusses the incremental pecuniary benefits for the state’s consumers in the main categories of incremental impact identified in the regulatory baseline.

3.1 How many consumers are impacted by the CCPA?

The personal information of all Californians is covered by the CCPA. According to the American Community Survey, there are 35M people in California that have internet access, either with a computer or a mobile phone. While the CCPA covers online and offline businesses, these online consumers will be the primary beneficiaries of the privacy protections afforded by the law.

3.2 Article 2 Benefits – Notice to Consumers

While the CCPA requires that businesses notify consumers about their CCPA rights, the proposed regulation establishes additional specifics regarding the format of these notifications. The incremental benefit of the regulation, therefore, includes the effects from the additional understanding of privacy rights *that would not have been achieved under notifications constructed without the regulation’s guidelines*. This additional understanding could lead to more consumers exercising their CCPA rights and, in turn, protecting their personal information which has a positive value to consumers. However, given all of the uncertainties, it is not possible to quantify the magnitude of this benefit.

3.3 Article 3 Benefits – Business Practices for Handling Consumer Requests

3.3.1 90-day Lookback Requirement

Article 3 specifies that if a consumer makes an opt-out of sale request, the business must notify any third party that was sold the consumer’s information in the past 90 days that the consumer has withdrawn their consent to sell the data. These third parties are then no longer allowed to sell the data further. The incremental benefit to consumers is stopping data sales among third parties to whom their data was sold in the past 90 days. The economic value of this benefit will depend on the value of the data types sold, the number of third party data transactions, and the number of consumers that request

businesses stop selling their data. However, because we do not have reliable information on the volume of third party data sales, it is not possible to quantify this benefit.

3.3.2 Training Requirements

The DOJ regulations specify that firms collecting, buying, selling, or sharing the personal information of more than 4 million California consumers must “establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business’s compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.” The benefit to consumers of additional business training will be an incrementally higher likelihood that businesses will follow the stipulations in the CCPA and that consumers’ personal information will be accurately given the protections provided by the CCPA.

3.3.3 Record Keeping

The regulation specifies additional record-keeping requirements for firms that collect, buy, sell, or share the personal information of more than 4 million California consumers. These businesses must compile a number of metrics on consumer requests and business responses from the prior year. The benefit to consumers is increased transparency with respect to business compliance of consumer requests to access, delete, and opt out of data sales. While this benefit is not easily quantifiable, the transparency requirements make it more likely that consumers’ requests to exercise their CCPA provided protections will be fulfilled completely and in a timely manner.

3.4 Article 4 Benefits – Verification of Requests

The regulation provides additional requirements for confirming the identity of consumers without accounts making CCPA requests. This will benefit consumers by limiting the possibility that someone posing as them gains access to or affects the privacy of their personal information through a fraudulent CCPA request. While this is expected to benefit consumers, the magnitude of the benefit is not easily quantifiable.

3.5 Article 5 Benefits – Special Rules Regarding Minors

The CCPA specifies that if a business collects personal information from minors to sell, the minor (if 13-16 years of age) or their parent or guardian (if under 13 years of age) must explicitly opt-in to the sale of that information. Article 5 of the proposed regulation specifies the process for opting-in. A benefit will accrue to minors who do not want their personal information sold, but who might have opted in with the CCPA (but without the proposed regulation), and who would not opt in under the proposed regulation. We do not have sufficient information on the number of minors in this group to quantify this benefit.

3.6 Article 6 Benefits – Non-Discrimination

The non-discrimination regulations proposed by DOJ attempt to clarify language in the CCPA about business practices that involve providing financial incentives or differential services/prices for consumers who exercise their rights under the CCPA. The CCPA directs DOJ to provide guidance to businesses regarding financial incentive offerings and the proposed regulation provides guidance on how businesses should calculate the value of consumer data for that purpose. The impact of the proposed regulation on consumers will therefore depend on the difference between how businesses would have calculated the value of consumer data absent the proposed regulation and how they will calculate the value of consumer data given the additional guidelines. Because businesses are allowed to charge consumers who exercise CCPA privacy rights for services at a price equivalent to the value of their personal information, we assume that the value of personal information calculated by businesses under the additional guidelines in the proposed regulation will be lower than they would have been absent the proposed regulation. If this is the case then the quantity of consumer benefits will be derived from the difference in prices charged with and without the proposed regulation. However, we do not have enough information to quantify this benefit.

4 Macroeconomic Impacts

4.1 Methodology

The economy-wide impacts of the proposed CCPA regulation will be evaluated using the BEAR forecasting model. The BEAR model is a dynamic computable general equilibrium (CGE) model of the California economy. The model explicitly represents demand, supply, and resource allocation across the California economy, estimating economic outcomes over the period 2015-2030. For this SRIA, the BEAR model is aggregated to 60 economic sectors, with detailed representation of the construction sectors most likely affected by the CCPA.

The current version of the BEAR model is calibrated using 2017 IMPLAN data for the California economy (BEAR: 2016b). Both the baseline and policy scenarios use the Department of Finance conforming forecast from June 2019. The conforming forecast provides assumptions on GDP growth projections for the State and population forecasts.

4.2 Scenarios

The macroeconomic impact results are based on the expected changes in compliance costs attributable to the *regulatory implementation of CCPA* (rather than the letter of the statute). The main scenario, *Proposed*, represents the expected impact on the overall California economy of this compliance. As discussed in previous sections, the direct CCPA compliance costs are subject to considerable uncertainty. We attempt to quantify the macroeconomic consequences of this uncertainty by considering three versions of the *Proposed* scenario, differing the scope of enterprise coverage. As in Table 2 above, we consider cases where 25%, 50%, or 75% of all California businesses that earn less than \$25 million in revenue will be covered under than CCPA. A survey completed by the International Association Privacy Professionals (IAPP) found that 8 out of 10 surveyed businesses believed that they would need to take compliance actions as a result of the CCPA. Because the survey went only to businesses in certain sectors likely to be covered by the law, the 50-75% upper-bound compliance range is reasonably supported by empirical evidence. Results for all scenarios are presented relative to the Baseline reference scenario that assumes CCPA law and pre-existing regulations remain in place.

Table 4 shows the direct costs that are measured for this analysis for the proposed regulation and the two regulatory alternatives. Costs are shown for all three methods of measuring how many firms may need to comply with the CCPA. These costs reflect total compliance spending over the entire analysis period (2020-2030) and have not been annualized. For the less stringent regulatory alternative, costs are approximately 25%

lower than the proposed regulations, regardless of how the number of compliant firms is measured. For the more stringent alternative, costs are 34%-39% higher than the proposed regulation.

Table 4: Decadal Compliance Costs For Proposed Regulation and Regulatory Alternatives (2020-30, \$ million)

	Low Firm Threshold	50% Firm Threshold	75% Firm Threshold
Proposed			16,454
Less Stringent	356	8,353	12,415
More Stringent	626	15,344	22,819

4.3 Inputs to the Assessment

In addition to the BEAR model’s detailed database on the Baseline structure of the California economy, the macroeconomic assessment is calibrated to incremental, sector-specific CCPA compliance costs as the primary inputs for the impact assessment (see Section 1.5). These compliance costs are broken into two categories: reflecting incremental costs for labor and technology. Labor costs pertain to compliance associated with operational planning costs and other human resource needs arising from CCPA, such as training and record-keeping. These costs will raise enterprise costs for skilled labor in each sector of the model that incurs CCPA compliance obligations. Technology costs are assumed to comprise 10% of CCPA costs attributable to design and/or purchases for technological infrastructure necessary to respond to consumer requests. These costs are modeled as an increase in sectoral purchases of goods and services from the information technology sector.

Cost for a representative scenario (50% firm compliance) and a representative year (2025) are shown in Table 5. While the macroeconomic model used for this analysis has 60 economic sectors, the table aggregates these costs to 2-digit NAICS codes for simplicity of exposition. Within NAICS codes, costs were allocated to BEAR sectors based on base year shares of output.

Table 5: Macroeconomic Inputs by Sector for a Representative Year (2025) and Scenario

Sector	Labor Cost		Tech Cost		Total Compliance Cost	
		% of Output		% of Output		% of Output
Agriculture, Forestry, Fishing, Hunting	0.870				2.480	0.004%
Mining, Quarrying, Oil-Gas Extraction	0.290	0.002%	0.530	0.003%	0.820	0.005%
Utilities	0.210	0.000%	0.390	0.001%	0.600	0.001%
Construction	32.680	0.017%	60.660	0.031%	93.340	0.048%
Manufacturing	16.950	0.002%	31.290	0.004%	48.240	0.007%
Wholesale Trade	24.120	0.011%	44.550	0.021%	68.670	0.033%
Retail Trade	32.550	0.018%	60.310	0.033%	92.860	0.051%
Transportation and Warehousing	9.400	0.008%	17.310	0.015%	26.710	0.023%
Information	41.510	0.004%	76.790	0.007%	118.300	0.011%
Professional, Scientific, and Tech Serv	55.900	0.013%	103.300	0.024%	159.200	0.037%
Educational Services	5.880	0.020%	10.890	0.037%	16.770	0.057%
Health Care and Social Assistance	42.330	0.018%	78.540	0.033%	120.870	0.051%
Arts, Entertainment, and Recreation	41.200	0.024%	76.410	0.045%	117.610	0.070%
Other Services (except Public Admin)	31.340	0.013%	58.180	0.024%	89.520	0.037%

4.4 Results

For the three comparison cases in our main, *Proposed* CCPA regulatory scenario, Table 6 presents impacts on the overall California economy over the period 2020-2030. A variety of macroeconomic metrics are listed, including real Gross State Product (GSP)⁷, total Full Time Equivalent state employment, gross state Output and Investment (at purchaser prices), and total Household Income. All financial indicators are discounted for inflation to a 2015 base year.

Although the magnitude of impacts varies over time and across comparison cases, the salient macroeconomic finding is that CCPA will impose small but consistently positive net costs on the economy. The simple reason for this is that CCPA compliance occasions costs for firms and other institutions that are not offset by pecuniary benefits to themselves or other California stakeholders. It must also be noted that we have made no attempt to

⁷ GSP is the state-level counterpart of GDP, or the total value added of all formal sector activities in the state economy.

value the benefits to consumers of these new protections, which could be considerable and would directly offset the net costs we present here. Thus, our net cost estimates are relatively pessimistic, but even in this case, it must be emphasized that the magnitude of these costs is very small in comparison to Baseline economic activity.

It is estimated (Table 6) that by 2030, California’s real GSP will be \$5.6 trillion dollars, meaning the largest impact in the most inclusive scenario (75% Threshold) would be (-4.6/5600<0.1%) less than one tenth of one percent of GSP. Although the relative magnitude of adjustment costs could be substantially higher for some groups and individual enterprises, the expected net total cost of CCPA is completely negligible in relation to the economy as a whole.

Table 6: Economy-Wide Impacts of CCPA Regulations
(billion\$ differences from baseline, 2015 dollars unless otherwise noted)

\$25 Million Revenue Threshold			
			2030
Real GSP		-0.110	-0.140
Employment (1,000 FTE)	-0.180	-0.310	-0.430
Real Output	-0.070	-0.120	-0.170
Investment	-0.030	-0.030	-0.040
Household Income	-0.040	-0.060	-0.080
50% Threshold			
			2030
Real GSP		-2.380	-3.090
Employment (1,000 FTE)	-4.550	-7.190	-9.520
Real Output	-1.560	-2.630	-3.740
Investment	-0.590	-0.690	-0.770
Household Income	-0.890	-1.310	-1.750
75% Threshold			
			2030
Real GSP		-3.530	-4.600
Employment (1,000 FTE)	-6.770	-10.690	-14.150
Real Output	-2.320	-3.900	-5.560
Investment	-0.880	-1.030	-1.140
Household Income	-1.320	-1.950	-2.610

More detailed examination of the main macroeconomic scenarios reveals that impacts vary in same direction as the scope of enterprise coverage, but not in a linear way. This is because the size distribution of California firms is quite heterogeneous. The \$25 million threshold qualifies only a small share of the state's enterprise population (the largest ones) for compliance. The two population share thresholds include many more and, as expected, moving compliance from 50% to 75% coverage raises aggregate adjustment costs by about half. Also intuitive is the intertemporal pattern of adjustment costs, which are basically rising with the Baseline expansion of the economy. These results indicate that aggregate impacts attributable to CCPA could not materially influence California's baseline growth dynamics. Again, however, this finding should not discount the importance of attention to adjustment needs for particular stakeholder groups such as small businesses.

5 Fiscal Impacts

An additional regulatory cost of the CCPA will come from staffing requirements needed to monitor compliance. Specifically, the DOJ has requested an additional 23 full time positions at an estimated cost of approximately \$4.5M per year. The DOJ currently enforces privacy rights through its Consumer Law Unit and Privacy Unit, a small subsection of attorneys comprised of one Supervising Deputy Attorney General (SDAG) overseeing four Deputy Attorney Generals (DAG). The CCPA will create new operational challenges in the enforcement of the framework that must be addressed through additional funding and staffing. To ensure adequate enforcement the DOJ has requested the following additional positions:

- Unfair Competition Law Fund
 - \$2,912,000 in FY 2019-20 and \$2,808,000 in FY 2020-21 and ongoing.
 - 9 Permanent Positions
 - 1 SDAG
 - 5 DAG
 - 3 Associate Governmental Program Analyst (AGPA)
 - \$250,000 annually for expert consultants
- General Fund
 - \$1,827,000 in FY 2019-20 and \$1,746,000 in FY 2020-21 and ongoing
 - 14 Permanent Positions
 - 3 DAG
 - 5 AGPA
 - 6 Legal Secretary
- Total Positions: 23
- Total Funding: \$4,739,000 in FY 2019 – 20, \$4,554,000 FY 2020 – 21 and ongoing

6 Economic Impacts of the Regulatory Alternatives

As required for major regulations, this SRIA considers two regulatory alternatives to the proposed regulation. For this analysis, the proposed scenario reflects results assuming DOF's projected growth rates for all relevant sectors.

First, a more stringent regulatory alternative considers an alternate approach to mandating a more prescriptive CCPA compliance pathway for eligible firms, by requiring more detailed training and record-keeping practices for all firms that must be compliance with CCPA. Second, a less stringent regulatory alternative would, among other things, allow limited exemption for GDPR-compliant firms. Limitations would be specific to areas where GDPR and CCPA are conformal in both standards and enforcement, subject to auditing as needed. This approach could achieve significant economies of scale in both private compliance and public regulatory costs.

6.1 More Stringent Regulatory Alternative

The economic impacts of the more stringent regulatory alternative are modeled by assuming that all CCPA-compliant firms are required to have staff dedicated to both training and record-keeping mandated in the proposed regulation for firms that handle the personal information of more than 4 million California consumers. This requirement would be an additional requirement (beyond the proposed regulations) for potentially hundreds of thousands of California businesses and would impose substantial costs.

Reasons for rejecting: DOJ rejects this regulatory alternative in order to ease the compliance burden for smaller businesses that would trigger a CCPA-compliance threshold but do not necessarily have the resources to devote additional staff to handle CCPA-related tasks. While the CCPA requires training and record-keeping, the proposed regulation does not require all firms to hire dedicated staff for this purpose. Larger firms that handle more consumer data would be subject to the stricter training and record-keeping regulations in order to ensure that they have dedicated individuals that are familiar with the CCPA and associated requirements.

6.2 Less Stringent Regulatory Alternative

The economic impacts of the less stringent regulatory alternative are modeled by assuming that a fraction of CCPA-compliant firms will not need to allocate additional resources to the technology and operational costs associated with CCPA since they can fully leverage their GDPR compliance systems. We assume that 25% of CCPA-regulated

firms would fall into this category. For these firms, training, recordkeeping, and other ongoing costs associated with the regulation are still assumed to apply.

Reasons for rejecting: DOJ rejects this regulatory alternative because of key differences between the GDPR and CCPA, especially in terms of how the scope of personal information is defined and the right to opt-out of the sale of personal information (which is not required in the GDPR). While GDPR-compliant firms will certainly be able to leverage much of their compliance program for CCPA, the privacy regulations and statutes are different enough that an exemption would not ensure that all consumer rights under the CCPA are properly accommodated.

6.3 Macroeconomic Impacts

Like the *Proposed* scenario results presented in Table 6, macroeconomic impacts for the Regulatory Alternatives were evaluated for the three comparison cases of enterprise inclusion. Unlike its predecessor, however, Table 7 presents results only for the year 2030. This is done for simplicity only, since the results are still monotone over time. Even though impacts are greatest in the final year, it is clear that they remain economically insignificant to California as a whole, regardless of the regulatory alternative chosen. This suggests that the merits of the choice should be institutional, reflecting the comments in Section 6.2, rather than economic. In other words, neither alternative has a compelling economic case, and thus the *Proposed* regulation is preferred.

Table 7: Economy-Wide Impacts of Proposed Regulation and Regulatory Alternatives in 2030
(billion\$ differences from baseline, 2015 dollars unless otherwise noted)

\$25 Million Revenue Threshold			
	Proposed Regulation	Less Stringent	More Stringent
Real GDP	-0.140	-0.100	-0.190
Employment (1,000 FTE)	-0.430	-0.290	-0.500
Real Output	-0.170	-0.120	-0.250
Investment	-0.040	-0.030	-0.050
Household Income	-0.080	-0.050	-0.100
50% Threshold			
	Proposed Regulation	Less Stringent	More Stringent
Real GDP	-3.090	-2.340	-4.670
Employment (1,000 FTE)	-9.520	-7.170	-12.520
Real Output	-3.740	-2.840	-6.140
Investment	-0.770	-0.580	-1.260
Household Income	-1.750	-1.320	-2.540
75% Threshold			
	Proposed Regulation	Less Stringent	More Stringent
Real GDP	-4.60	-3.48	-6.95
Employment (1,000 FTE)	-14.15	-10.66	-18.61
Real Output	-5.56	-4.21	-9.13
Investment	-1.14	-0.86	-1.88
Household Income	-2.61	-1.97	-3.78

7 Summary of Economic Results

Assessment of the CCPA regulation indicates that it will have consistently positive net costs for the state economy, but the magnitude of these costs is negligible from a macroeconomic perspective. Certainly, more specific stakeholder groups, individual firms, and others, can be expected to face important adjustment costs, and complementary policies regarding special adjustment needs are worthy of consideration. Having said this, however, the overall impact estimated here for CCPA, excludes valuation of many offsetting non-pecuniary benefits and is therefore relatively pessimistic. The resulting impact amounts to a tiny fraction of overall economic activity.

For a regulation of CCPA's consequence for the state and one of its leading knowledge intensive industries, the direct costs present a notable, but hardly insurmountable challenge. For most other activities across this large and highly diversified and robust economy, impacts of CCPA will be nearly imperceptible.

With respect to regulatory alternatives, this SRIA presents two leading candidates with supporting and dissenting arguments for each. The estimates presented for these alternative scenarios indicate that economic differences between the policies, like the total impacts of the *Proposed* policy, are economically insignificant to California as whole. In other words, neither alternative has a compelling economic case, and thus the *Proposed* regulation, which offers significant benefits at reasonable costs, is preferred.

8 References

- A.P.C., Kotterink, B., and S. Marcus. "Data Protection Review: Impact on EU Innovation and Competitiveness". Report carried out at request of the European Parliament's Committee on Industry, Research, and Energy (ITRE). December 2012.
- BEAR (2016a). "Review of Standardized Regulatory Impact Assessments to Date." Report prepared for the California Energy Commission.
- BEAR (2016b). "Berkeley Energy and Resources (BEAR) Model: SRIA Baseline Forecast for the California Economy." Report prepared for the California Energy Commission.
- BEAR (2016c). "Economic Assessment for SB350: Economic Analysis." Report prepared for the California Independent System Operator, Volume 8, <http://bearecon.com/portfolio-item/caiso-sb350/>
- BEAR (2016d). "Economic Assessment for SB350: Disadvantaged Community Impacts." Report prepared for the California Independent System Operator, Volume 10, <http://bearecon.com/portfolio-item/caiso-sb350/>
- Cave, J., Schindler, H.R., Robinson, N., Horvath, V., Castle-Clarke, S., Roosendaal, Christensen, L., Colciago, A., Etro, F., and G. Raftert "The Impact of the Data Protection European Commission. "Impact Assessment: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)". Brussels, 25.1.2012.

- Ferracane, M.R., Kren, J., and E.V. Marel "Do Data Policy Restrictions Improve the Productivity Performance of Firms and Industries?". European Centre for International Political Economy DTE Working Paper 01. 2019.
- IMPLAN, REMI, and RIMS II: Benchmarking Ready-Made Models for Comparison." *The Annals of Regional Science* 29 (4): 363–74.
- Madden, Mary and Lee Rainie. "Americans' Attitudes About Privacy, Security, and Surveillance." Pew Research Center, 2015.
- Purcell, Kristen, Joanna Brenner, and Lee Rainie. "Search Engine Use 2012." Pew Research Center's Internet & American Life Project, 2015.
- Regulation in the E.U." Intertic Policy Paper. Intertic 2013.
- Rickman, Dan S., and R. Keith Schwer. 1995. "A Comparison of the Multipliers of Roland-Holst, David. "Cap and Trade and Structural transition in the California Economy," Research Paper 0707121, Center for Energy, Resources, and Economic Sustainability, University of California, Berkeley, September, 2007.
- S. J. Savage and D. M. Waldman. Privacy tradeoffs in smartphone applications. *Economics Letters*, 137:171–175, 2015.
- Savage S.J., D.M. Waldman "Privacy tradeoffs in smartphone applications." *Economics Letters*, 137:171–175, 2015.
- Scott, Mark, Laurens Cerulus, and Steven Overly (2019). "How Silicon Valley gamed Europe's privacy rules." POLITICO. <https://www.politico.eu/article/europe-data-protection-gdpr-general-data-protection-regulation-facebook-google/>
- Short J.E., S. Todd (2017) What's Your Data Worth? MIT Sloan Management Review, 58 (3).

Short, J.E. and S. Todd. What's Your Data Worth? MIT Sloan Management Review, 58 (3). 2017.

Steele E., Locke C, Cadman E, Freese, B. "How much is your personal data worth?" Financial Times, 2013. Available at <https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2z2agBB6R>

TrustArc. "CCPA and GDPR Compliance Report," 2019. Available at https://info.trustarc.com/Web-Resource-2019-03-18-CCPA-GDPRComplianceReport_LP.html

U.S. Census Bureau. Census 2010 Supplementary Survey (C2SS). Washington, D.C.: U.S. Bureau of the Census (2015).

APPENDIX B

(Department of Finance's Comments)

Stacey Schesser
Supervising Deputy Attorney General
California Department of Justice
455 Golden Gate Ave., Ste. 11000
San Francisco, CA 94102

September 16, 2019

Dear Ms. Schesser:

Thank you for submitting the standardized regulatory impact assessment (SRIA) and summary (Form DF-131) for the California Consumer Privacy Act proposed regulations, as required in California Code of Regulations, title 1, section 200(a)(1) for major regulations.

The SRIA assumes that the proposed regulations are limited to the minimum systemic requirements for notification of data collection and data removal mechanisms by businesses, potentially affecting more than half a million California businesses and the information of 35 million internet users with a value of at least several billion. Depending on the size of the firm, the cost of compliance can range from a one-time cost of \$50,000 to over \$2 million for larger firms with business models that heavily exploit personal data. The SRIA estimates that the initial cost of compliance may be up to \$55 billion. However, given that many of the larger California firms affected are competitive worldwide and may have had to comply with the EU data regulations, the change in their business models and profits may be smaller. The value of a person's data is more difficult to estimate, as a detailed picture can be much more valuable once assembled from individual pieces that firms collect. The SRIA estimates that this may total up to \$10 billion each year for the sensitive personal information of California internet users.

In general, Finance concurs with the methodology used to estimate impacts of proposed regulations. The SRIA clearly lays out for the public the proposed regulatory impacts, and does a good job of showing how this proposed regulation may change how individuals and businesses interact in California. However, the SRIA does not address the longer-term benefits to competition, the ability of consumers to refuse increasingly targeted price discrimination, and an economic system that relies on people being able to reinvent themselves, as these are difficult to quantify. In addition, the impacts of privacy protections will depend on changing consumer awareness and preferences, and we expect that these will be addressed in impact assessments of future regulatory packages.

These comments are intended to provide sufficient guidance outlining revisions to the impact assessment if a SRIA is required. The SRIA, a summary of Finance's comments, and any responses must be included in the rulemaking file that is available for public comment. Finance understands that the proposed regulations may change during the rulemaking process. If any

significant changes to the proposed regulations result in economic impacts not discussed in the SRIA, please note that the revised economic impacts must be reflected on the Standard Form 399 for the rulemaking file submittal to the Office of Administrative Law. Please let us know if you have any questions regarding our comments.

Sincerely,

A handwritten signature in blue ink, appearing to read "Irena Asmundson".

Irena Asmundson
Chief Economist

cc: Mr. Lenny Mendonca, Director, Governor's Office of Business and Economic Development
Mr. Kenneth Pogue, Director, Office of Administrative Law
Mr. Sean McCluskie, Chief Deputy, California Department of Justice