Computer & Communications
Industry Association
Tech Advocacy Since 1972

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Via email: PrivacyRegulations@doj.ca.gov

Re: *Computer & Communications Industry Association comments on California Consumer Privacy Act proposed regulations*

Dear Privacy Regulations Coordinator:

Thank you for the opportunity to comment on the Attorney General's proposed implementing regulations for the California Consumer Privacy Act of 2018 (CCPA). The Computer & Communications Industry Association (CCIA) is an international nonprofit trade association representing a broad cross section of large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[1]

CCIA members place a high value on protecting consumer privacy and support the consumer rights and privacy principles that underpin the CCPA including transparency, notice, and consumer control over data processing practices.[2] However, the hurried and haphazard process that led to the enactment of the CCPA produced many areas of unintended complexity, contradiction, and lack of clarity. While some of these shortcomings have been addressed through subsequent legislative amendments to the Act, the Attorney General's regulations should focus on providing additional clarity and guidance to businesses in order to ensure manageable compliance with the CCPA. CCIA welcomes the thoughtful and deliberative approach taken by the Attorney General's office in developing the draft implementing regulations. We believe that with certain modifications, these regulations can set consistent expectations for consumers and businesses of their rights and obligations under the CCPA in order to promote consumer privacy rights within California.

[1] A complete list of CCIA's members is available online at www.ccianet.org/members.

[2] CCIA, *Privacy Principles: A New Framework for Protecting Data and Promoting Innovation* (Nov. 7, 2018), http://www.ccianet.org/wp-content/uploads/2018/11/CCIA_Privacy_Principles.pdf.

The following comments were developed through discussion with CCIA's member companies and reflect clarifications and amendments to the proposed regulations that will support reliable operationalization of the rights and obligations established by the CCPA. The following comments are comprised of general observations on the draft regulations as well as recommendations for specific amendments to the text of the regulations.

General Comments on the Draft Regulations

The draft regulations add much needed clarity to certain aspects of the CCPA; however, areas of confusion remain. CCIA encourages the Attorney General's office to consider the following high-level points in revising the draft regulations in order to provide additional clarity, establish harmony with existing best practices, promote interoperability with other applicable laws, account for recent statutory amendments, and remain consistent with California law.

1. The draft regulations add much needed clarity: CCIA welcomes provisions in the draft regulations that provide additional clarity and guidance for complying with previously ambiguous components of the CCPA. For example, the draft regulations pertaining to the treatment of "household" data (§ 999.318), the ability to offer granular options for exercising deletion requests (§ 999.313(d)(7)), and procedures for the verification of consumer requests (§ 999.323) are important additions that should be retained in the final implementing regulations.

2. Areas of confusion remain and should be addressed: The rushed legislative process that produced the CCPA resulted in unclear provisions that are not fully addressed or clarified by the draft regulations. The final regulations should provide additional clarity and appropriate flexibility for vague and undefined terms and concepts used by the CCPA in accordance with common legal understanding and usage of these terms. For example, the regulations should clarify the meaning of "valuable consideration" and "reasonable security procedures and practices" as used in the CCPA.[3] Such clarifications are necessary to prevent overbroad interpretations of the law that could disrupt the basic operation and availability of websites and online services.

3. Follow best practices for privacy notices and policies: CCIA supports enabling flexibility in meeting privacy notice requirements to support the development of concise and

[3] CCPA §§ 1798.140(t)(1); 1798.150(a)(1).

effective notices in different contexts.[4] Where appropriate, businesses should be empowered to utilize modern tools such as privacy dashboards, layered notices, and inline videos and controls in order to provide streamlined and effective notice of data processing practices. The prescriptive, repetitive, and lengthy new privacy notice and policy requirements contemplated by Article 2 of the draft regulations would increase costs, contribute to ballooning notice length, and potentially lead to consumer fatigue - reducing the overall effectiveness of the CCPA's efforts to meaningfully inform consumers of businesses' data practices. In promulgating final CCPA regulations, the Attorney General should consider ways to promote concise, relevant, and effective transparency of businesses' data processing practices.

4. Promote interoperability between privacy regimes: Where appropriate under the authority of the CCPA,[5] the regulations should define terms, clarify obligations, and establish exceptions in a manner that promotes interoperability and harmonization with intersecting state (e.g., the California Online Privacy Protection Act (CalOPPA)), federal (e.g., the Children's Online Privacy Protection Act (COPPA)), and international (e.g., the General Data Protection Regulation (GDPR)) privacy laws. Supporting the emergence of a "common language of privacy"[6] will promote reliability and predictability for businesses in meeting their CCPA obligations and consumers exercising their rights.

5. Account for recent CCPA amendments: The final regulations should account for and operationalize the CCPA amendments signed by Governor Newsom on October 11, 2019. Specifically, the regulations should be updated in response to changes pertaining to exceptions for employee and business-to-business data (AB 1335, 25), methods for receiving consumer requests (AB 1546), and the definition of "personal information" (AB 874).[7]

6. Ensure regulations are authorized by statute and provide clarity: Pursuant to the California Administrative Procedure Act (Cal. Gov't Code § 11340) and associated case law (*see Morris v. Williams*)[8], the Attorney General should avoid creating new substantive requirements for businesses through the regulatory process that are outside

[4] *See e.g.*, Information Commissioner's Office, *What methods can we use to provide privacy information?*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information (last visited Dec. 2, 2019).
[5] CCPA § 1798.185(a)(3).
[6] *See* NIST, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* (Sept. 6, 2019), https://www.nist.gov/system/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf.
[7] *See* Privacy & Information Security Law Blog, *California Governor Signs CCPA Amendments Into Law* (Oct. 13, 2019), https://www.huntonprivacyblog.com/2019/10/13/california-governor-signs-ccpa-amendments-into-law.
[8] *Morris v. Williams*, 67 Cal. 2d 733 (1967) ("Administrative regulations that alter or amend the statute or enlarge or impair its scope are void and courts not only may, but it is their obligation to strike down such regulations.").

the scope of the CCPA unless clearly authorized and necessary to operationalize an express statutory right or specified legislative purpose. The legislative intent in enacting the CCPA was to give "consumers an effective way to control their personal information" by ensuring a series of rights such as knowledge, access, ability to say no to sale, and nondiscrimination.[9] Any substantive additions to business obligations should have a concrete link to furthering the CCPA's purpose of promoting consumers' effective control of their personal information through the exercise of these rights.

Comments on Specific Regulatory Language

CCIA respectfully offers the following analysis and suggested amendments to specific provisions of the draft regulations in order to promote clear and effective operationalization of the rights and business obligations established in the CCPA.

Draft Regulation § 999.305(a)(3)

- Analysis: Obtaining explicit consent for any data processing not disclosed through an initial notice, no matter how beneficial or benign, would be a burdensome requirement that is inconsistent with best practices.[10] Such a requirement could obstruct businesses from adapting to emerging business practices, limit innovation, and restrict socially beneficial secondary data uses. Furthermore, the requirement could motivate some businesses to draft overbroad privacy notices for the point of initial collection, limiting the effectiveness of these notices for meaningfully informing consumers of data processing practices. Finally, this regulation would constitute a substantive restriction that is not contemplated by the CCPA or addressed in the CCPA's legislative intent. While the Attorney General's Initial Statement of Reasons (ISOR)[11] posits that this requirement would "implement" CCPA § 1798.100(b), that provision only restricts businesses from using personal information for additional purposes without first "providing the consumer with *notice* consistent with this section" (emphasis added).[12] Therefore, this regulation should be limited to providing guidance to businesses on how to notify consumers on the use of personal information for new purposes as directed by the CCPA.

[9] CCPA Legislative Counsel's Digest, Sec. 2.(i); *see also* California Attorney General, *Initial Statement of Reasons: Proposed Adoption of California Consumer Privacy Act Regulations* (ISOR) II, *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

[10] *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, at 57 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("Companies should obtain affirmative express consent before making *material retroactive* changes to privacy representations.").

[11] ISOR IV.C. subdivision (a)(3)-(4).

[12] CCPA § 1798.100(b).

- Proposed language: § 999.305(a)(3) A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection **without**~~.~~ ~~If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall~~ directly notify**ing** the consumer of this new use **through the business's primary means of contact with the consumer.** ~~and obtain explicit consent from the consumer to use it for this new purpose~~.

Draft Regulation § 999.306(d)(2)

- Analysis: The draft regulations contain a necessary exemption from providing a notice of the right to opt-out if a business does not sell personal information. However, the requirement that a business using this exemption must include in its privacy policy a statement that it "does not and *will not sell personal information*" should be amended. A business that does not sell consumer data may, at some point in the future, decide to begin selling consumer data (consistent with CCPA requirements) in response to shifting business practices, technology, or consumer/client requests. If a business that chooses to 'sell' personal information (as broadly defined by the CCPA) has previously stated that it will never sell any personal information in accordance with this draft regulation, it could be subject to claims of deceptive practices under FTC Section 5 or equivalent State authority. The ISOR demonstrates that the Attorney General's office intends for companies that do not sell personal information not to provide opt-out notices in order to avoid "potentially confusing" consumers.[13] Therefore businesses should be able to exercise this exemption without being required to make potentially misleading statements in doing so.

- Proposed language: § 999.306(d)(2) It states in its privacy policy ~~that~~ that it does not ~~and will not~~ sell personal information. A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out.

Draft Regulation § 999.313(c)(4)

- Analysis: As the ISOR recognizes, the Attorney General's office has an important task of balancing the significant benefits of consumers' right to access their personal information while also limiting the potential harms that may result from the inappropriate disclosure of information.[14] The draft regulations appropriately bar the disclosure of certain categories of information in response to a request to know, such as account passwords and security question answers due to the serious risks that could result from inappropriate

[13] ISOR IV.D. subdivision (d).

[14] ISOR IV.H subdivision (c)(4).

disclosure. However, the draft regulation's contemplated ban on the disclosure of any government-issued identification number is overbroad and contrary to consumer interests. For example, consumers may expect the right to access, and benefit from the ability to port to different services, certain documents containing identifiers such as medical forms or tax return documents that would not have the same utility if the identifiers were removed. Given that the CCPA does not establish or suggest a blanket ban on such disclosures, but rather instructs the Attorney General to establish rules facilitating consumers' ability to obtain their covered information,[15] the draft regulations should be amended to permit the disclosure of identification numbers in order to fulfill a verified request that does not carry an otherwise unreasonable risk.

- Proposed Language: § 999.313(c)(4) **Taking into account the context and purpose of a consumer's request,** a business **may choose to** ~~shall not at any time~~ disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, **or** any health insurance or medical identification **in response to a verified request to know. A business shall not at any time disclose** an account password or security questions and answers.

Draft Regulation § 999.313(d)(1)

- Analysis: The draft regulation appropriately recognizes that businesses must have the ability to deny unverifiable data deletion requests. However, requiring businesses to treat an unverifiable deletion request as an opt-out of sale is not supported by the CCPA and raises both practical and policy concerns. First, any such requirement would need an additional exception for instances that a business is unable to associate the unverifiable deletion request with a customer or user account. Second, deletion requests are substantively different from opt-out of sale requests and mandating the transformation of the former into the latter does not necessarily "best accommodate"[16] the consumer's intent. For example, a customer may wish to delete discrete categories of personal information pursuant to draft regulation § 999.313(d)(7), but not wish to opt-out of sales in order to take advantage of a price difference offered pursuant to draft regulation § 999.336(b). Due to these concerns, the Attorney General should remove this requirement from the draft regulations.

- Proposed language: § 999.313(d)(1) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified~~ and shall instead treat the request as a request to opt-out of sale~~.

[15] CCPA § 1798.185(a)(7).

[16] ISOR IV.H subdivision (d).

Draft Regulation § 999.314(c)

- Analysis: In order to support legislative intent and promote interoperability between different privacy regimes, the regulations should align the scope and obligations of "service providers" under the CCPA with those of "data processors" under the GDPR and standard business contractual relationships.[17] Unfortunately, the draft regulation's provisions on the use of covered information by service providers is overly restrictive and could be construed to limit legitimate business practices necessary to conduct business or provide a service. The draft regulation creates a new legal distinction for combining personal information that is not contemplated in the CCPA's differentiation between a service provider's "business purposes" and "commercial purposes."[18] The regulations should be modified to permit the use of combined data for all appropriate cybersecurity practices (not just the relatively narrow "detection" of "data" security incidents), operational purposes such as product analysis and improvement, and additional business purposes that rely on pooling information to provide a common service to the benefit of all customers.

- Proposed language: § 999.314(c) A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity **unless the service provider's business purpose provides a common benefit to all customers**. A service provider may~~, however,~~ **also** combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to **prevent,** detect**, and respond to** ~~data~~ security incidents,~~ or~~ protect against fraudulent or illegal activity**, or for operational purposes such as auditing, account maintenance, and conducting measurement or improvement of the service**.

Draft Regulation § 999.314(d)

- Analysis: Under the CCPA, a service provider is not "liable" for the "obligations of a business for which it provides services."[19] However, the proposed regulations would create a new obligation for service providers to either comply with consumer CCPA requests or to explain the basis for their denial. It is inappropriate to create an expectation for service providers to comply with consumer access and deletion requests unless pursuant to a contract entered into between business partners. Typically, service

[17] The CCPA's definition of "service provider" under § 1798.140(v) closely tracks the GDPR's definition of "processor" under GDPR Art (4)(8).

[18] CCPA § 1798.140(d), (f).

[19] CCPA §1798.145(j), Certain indirect obligations under §1798.104(c)

providers have a duty to maintain the integrity of the data of a business and are not in the best position to verify consumer requests or to determine whether an exception applies. Furthermore, as the ISOR recognizes, the CCPA does not oblige service providers to comply with consumer requests,[20] so it is unclear what additional, meaningful information is expected to be included in a service provider's basis of denial. As stated, the regulations should align the obligations of service providers with the GDPR, which requires that data processors assist data controllers with responding to data subject rights, but does not require compliance with consumer requests or direct responses.[21]

- Proposed language: § 999.314(d) If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services **and is not contractually obligated to respond**, ~~and does not comply with the request, it shall explain the basis for the denial. T~~**t**he service provider shall ~~also~~ inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information~~ and, when feasible, provide the consumer with contact information for that business~~.

Draft Regulation § 999.315(c)

- Analysis: The CCPA establishes specific mechanisms for consumers to exercise control over their personal information, including by opting-out of the sale of their personal information through the use of a clear and conspicuous "Do Not Sell My Personal Information" link or a uniform opt-out logo or button.[22] Therefore, while the CCPA envisions uniformity in opt-out request mechanisms, in contrast, the proposed regulations would provide for the creation of a limitless amount of divergent, yet-to-be-developed opt-out methods. Internet communications are based upon open, consensus-based protocols and standards. It would be impractical to demand that businesses continually update their websites and servers to detect and enable compatibility with an ever-expanding array of different browser extensions, plug-ins, and other signifiers that might be intended to convey opt-out requests. In order to ensure that consumers can meaningfully exercise their privacy controls and grant certainty to businesses in receiving and responding to consumer requests under the CCPA, this provision should be removed.

Draft Regulation § 999.315(f)

- Analysis: Requiring businesses that receive an opt-out request to notify all third parties to whom it sold the personal information of a consumer within the past 90 days and instruct

[20] ISOR IV.I subdivision (d).

[21] GDPR Art. 28(3)(e).

[22] CCPA §§ 1798.135(a)(1); 1798.185(a)(4)(C).

them not to further sell the information would be a burdensome requirement not contemplated by the text of the CCPA. Furthermore, such a requirement is impractical in the modern information economy where data transfers without a backwards-looking mechanism occur for various legitimate business purposes. Complying with this provision would require that businesses conduct additional tracking, collection, and retention of personal information, contrary to privacy best practices and in tension with draft regulation § 999.317(f) clarifying that "a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made user the CCPA." [23] Furthermore, the draft regulation is unclear as to how an instruction "not to further sell the information" shall be enforced. Given these concerns it is appropriate to include a feasibility exception in this provision, as is included elsewhere in the draft regulations.

- Proposed language: § 999.315(f) **Where feasible,** ~~A~~ **a** business shall 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 consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. ~~The business shall notify the consumer when this has been completed.~~

Draft Regulation § 999.317(g)

- Analysis: The draft regulations propose to create a new, inherently arbitrary distinction between businesses that collect the personal information of 4,000,000 or more consumers and those that do not, placing additional obligations on the former category that are not required by the CCPA and have no clear connection to furthering the ability of consumers to control their personal information. The inclusion of metrics about consumer requests within an organization's privacy policy would lengthen and complicate these notices, in all likelihood decreasing their utility at meaningfully informing consumers of data processing practices. Furthermore, there is no legitimate basis for requiring costly training programs to ensure that an employee who only touches one aspect of CCPA compliance, such as handling consumer access or deletion requests, must be informed of entirely distinct CCPA provisions such as the business's information security obligations under the Act. The ISOR states that this training requirement is intended to ensure that businesses "are capable of adequately responding to these requests,"[24] however, mandating businesses offer training on topics wholly unrelated to consumer requests under the CCPA would not advance this purpose.

[23] *See also* CCPA § 1798.145(k) ("This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business") (as amended by AB 1355).

[24] ISOR IV.L subdivision (g).

Finally, the draft provision is unclear as to whether it applies to businesses that process records of 4 million or more total individuals or 4 million Californians.[25] This is a serious oversight given the impending effective date of the CCPA. Considering these fundamental shortcomings, this draft provision should be removed from the regulations.

Draft Regulation § 999.330

- Analysis: The CCPA creates obligations regarding the sale of personal information of minors if the business has "actual knowledge" of the age of the consumer.[26] However, this standard is only described in the draft regulations through a negative proposition - that a business will be deemed to have "actual knowledge" if it "willfully disregards the consumer's age."[27] Given that the phrase "willfully disregards" is not used in the CCPA or defined in the draft regulations, this provision could be read as requiring businesses to investigate the age of its users by collecting and associating additional personal information, in contradiction of well-established best practices for privacy. In order to provide clarity for businesses, the regulations should explicitly state that the meaning of "actual knowledge" in the CCPA is equivalent to longstanding FTC guidance on the "actual knowledge" standard under COPPA.[28] This clarification is appropriate given that the ISOR repeatedly indicates the Attorney General's intent to align CCPA provisions pertaining to minors under 13 with equivalent provisions in COPPA.[29]

- Proposed language: **§ 999.330(c) The "actual knowledge" standard has the same definition and scope as used by the Children's Online Privacy Protection Act. Nothing in these regulations will be interpreted as requiring a business operating a website or online service to investigate or inquire about the age of a visitor or user.**

Draft Regulation § 999.336(a)

- Analysis: The draft regulations establish that a "service difference is discriminatory" and prohibited by the CCPA if the business "treats a consumer differently because the consumer exercised a right conferred by the CCPA." The regulations should recognize that in certain cases the exercise of a right under the CCPA, such as the right to deletion, will necessarily cause a service difference if the service is based on data the business

[25] While the draft regulations state that these obligations apply to businesses that process the "personal information of 4,000,000 or more consumers" (§ 999.317(g)), the ISOR states that this distinction was selected on the basis that these businesses "handle the personal information of a significant portion of California's population" (ISOR IV.N subdivision (g)).
[26] CCPA § 1798.120(c).
[27] *Id.*
[28] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (Mar. 20, 2015) at A.14, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.
[29] ISOR IV.R.

processes related to the consumer. For example, a service that recommends content based on past user engagement and ratings will necessarily offer less relevant content if a consumer exercises their right to delete that information. More fundamentally, a business would no longer be capable of charging for a subscription-based service if a consumer deletes their billing information.

- Proposed language: § 999.336(a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations **unless the exercise of that right affects the ability of the business to offer the service**.

Draft Regulation § 999.337

- Analysis: CCIA appreciates the flexible approach to calculating the value of a consumer's data set out by the draft regulation and the ISOR's recognition that "there is not a single generally accepted methodology for calculating the value of a consumer's data."[30] However, as the value of data is primarily derived from inferences based upon the aggregation of information, not upon any individual datum, calculating the value of consumer data remains a largely subjective and amorphous practice.[31] It is unclear under the CCPA, regulations, and ISOR how a business is expected to defend its data valuation approach if challenged.

Thank you again for the opportunity to comment on the draft implementing regulations for the California Consumer Privacy Act. If you have any questions regarding the comments and recommendations in this letter, please contact Keir Lamont, Policy Counsel, at klamont@ccianet.org.

Sincerely,

Keir Lamont
Policy Counsel
Computer & Communications Industry Association

[30] ISOR at IV.V.

[31] *See* Will Rinehart, *Testimony to the Committee on Banking, Housing, and Urban Affairs Hearing on Data Ownership*, American Action Forum (Oct. 24, 2019), https://www.americanactionforum.org/testimony/hearing-on-data-ownership-exploring-implications-for-data-privacy-rights-and-data-valuation.