Message

From: Paul Ruden [redacted]
Sent: 12/6/2019 5:37:35 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: California Consumer Privacy Act Regulations
Attachments: CCPA comment.docx

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

The undersigned submits the attached comments in the docket for the proposed adoption of sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations (CCR) concerning the California Consumer Privacy Act (CCPA).

Paul M. Ruden
Principal
Paul M Ruden Consutling

PAUL M. RUDEN CONSULTING

[redacted]

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

The undersigned submits these comments on the Notice of Proposed Rulemaking Action published at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf in implementation of the California Consumer Privacy Act (CCPA).

These comments are focused on an important jurisdictional question raised by, but not discussed in, the proposed regulations.

The CCPA is expressly directed at for-profit businesses that have: 1) $25 million or more in annual revenue; 2) trade in the data of 50,000 or more persons; or 3) derive 50% or more revenue from selling consumers' personal information. The "consumers" whose data is covered by the CCPA are "natural persons" residing in California, thus excluding data of corporations. In addition to the size factors, the CCPA will only apply if the business collects *and* processes the personal information of California residents *and* does business in the State of California.

The regulations are clear that the intent is to also bind non-California businesses that acquire personal information about California residents:

> "... out-of-state competitors would also be subject to the CCPA and the regulations for their California customers." [Notice of Proposed Rulemaking Action at 13]

This raises the important question of how much business must be done with "California customers" to bring the regulations to bear on non-resident businesses.

The proposed regulations and the economic impact analysis do not directly address this question. I submit that the law prevents California from treating out-of-state businesses more aggressively than in-state competitors. Therefore, the same three thresholds for enforcement of the statute should apply to out-of-state businesses that sell to California residents and the thresholds ($25 million in revenue, for example) should be construed to refer to business with California residents and not business done elsewhere.

The Standardized Regulatory Impact Assessment (SRIA) is consistent with the interpretation I have proposed. It references "consumers" and thus refers to "natural persons" residing in California." Nevertheless, a jurisdictional question of this nature should not be left to interpretation. It will be a simple matter to make the suggested application of the regulations explicit in the final regulation.

Clarification of this issue in the final regulations is critical so that non-California firms can understand exactly how to assess their business operations regarding compliance with the CCPA.

Respectfully submitted,

/Paul M. Ruden/

Paul M. Ruden
Principal
Paul M Ruden Consulting

Message

From:	Alkhasyan, Karina [redacted]
Sent:	12/6/2019 10:40:48 PM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC:	Bonnay, Julien [redacted]; Vishnu, Sandeep B [redacted]; Vijayakrishnan, Jayadevan [redacted]
Subject:	Capco - CCPA Proposed Commentary
Attachments:	CCPA - Comments_20191205.pdf

Good evening,

On behalf of Capco's Cybersecurity and Data Privacy practices, please see several aspects of the existing California Consumer Protection Act text we believe may require additional clarification to ensure that businesses are equipped with the adequate information to comply with the requirements.

Our detailed comments are outlined in the attached PDF and below you will find a brief summary of the requested clarification points:

1. Considerations for technical limitation related to data purge requests
2. Data retention period for PI
3. Thresholds for the determination of "reasonable need" for refusal of customer requests to purge data
4. Methodology for determination of cost / value of customer PI
5. Accountability for the risk of transmitting PI over unencrypted / unsecure networks

For some background information, Capco is a management consulting firm that works with leading financial services institutions to address challenges related to cybersecurity and data privacy, among others.

Thank you for your consideration.

Best regards,
Karina Alkhasyan
Senior Consultant
CAPCO | 77 Water Street | New York | New York | 10005
W: www.capco.com
[redacted]

CAPCO
THE FUTURE. NOW.

CCPA CLARIFICATION PROPOSAL

THE FOLLOWING KEY POINTS MAY REQUIRE FURTHER CLARIFICATION FROM THE REGULATORY BODY

Capco is a management consultancy working with leading financial institutions on strategic topics including but not limited to cyber security and data privacy. Based on our discussions with several clients, we see 5 areas that could benefit from clarifications:

1	**TECHNICAL LIMITATIONS**	Recourse / direction for financial institutions faced with technical limitations in purging personal information
2	**DATA RETENTION PERIOD**	Limitations on the age of data which clients are able to request a business to purge
3	**REASONABLE NEED**	Quantitative thresholds for considerations of what is "reasonable need" to justify refusal to delete client data
4	**COST OF PII**	Methodology for determining the cost / value of PI to justify reasonable need / value if breached.
5	**ACCOUNTABILITY FOR CONFIDENTIALITY RISK**	Body responsible for the risks associated with potential breach of PI data in transit due to communication over an unencrypted / potentially compromised network.

Message

From: Keir Lamont [redacted]
Sent: 12/6/2019 1:13:50 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCIA comments on the CCPA proposed regulations
Attachments: [CCIA] Comments on CCPA draft regulations.pdf

Dear Privacy Regulations Coordinator:

Please find attached the comments of the Computer & Communications Industry Association on the draft implementing regulations for the CCPA.

Best regards,
Keir Lamont

--
Keir Lamont
Policy Counsel
Computer & Communications Industry Association (CCIA)
[redacted]

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~~the 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 [redacted]

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.

Message

From: James Harrison [redacted]
Sent: 12/7/2019 12:57:48 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCP Comments on Draft Regulations
Attachments: CCP Letter to AG re Proposed Regs (00396582-3xAEB03).docx

Attached please find the comments of Californians for Consumer Privacy on the Attorney General's draft regulations implementing the CCPA. We also suggest removal of the following as they would still pose a risk to consumers form misuse and breach, and contrary to what an average consumer would understand as their right to delete.

1. De-identifying the personal information; or
2. Aggregating the personal information.

Thank you for your consideration.

James Harrison

James C. Harrison
Remcho, Johansen & Purcell, LLP
1901 Harrison Street, Suite 1550
Oakland, CA 94612
[redacted]
www.rjp.com

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication

CALIFORNIANS FOR
CONSUMER PRIVACY

November 19, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

To Whom It May Concern:

Thank you for the opportunity to offer comments regarding the Attorney General's proposed regulations to implement the California Consumer Privacy Act ("CCPA"). We are grateful to the Attorney General's Office for the thoroughness and thoughtfulness of the proposed regulations, and we are generally supportive of proposed regulations but we have a few suggestions we believe will better adhere to the spirit and intent of the law:

> **1. Notice at Point of Collection:** Section 999.305(a)(2)(e) and (b)(3), and Section 999.306(b)(2), set forth the notice requirements when businesses collect consumers' personal information. The regulations should clarify that when a business collects a consumer's personal information while a consumer is physically present at or near the business's premises, such as by collecting information from the consumer's device while the consumer wanders through a store and stops to examine items, or when the consumer is walking by a trash can outside, then the notice requirements should include a detailed, physical notice at the point of collection, specifying what is happening to a consumer's personal information, rather than a notice that is limited to a web address where consumers can get information. Much like a health rating in a restaurant window, this information should be readily available to consumers at the location at which the interaction occurs, rather than simply being available to consumers who take the time to visit a website while physically present on the business's premises.
>
> If restaurants only had to post a web address on their inspection notices, many consumers would not take the time to visit, which is why health agencies require the notice be 10" tall and visible from a distance.
>
> We propose the following language in Section 999.305(a)(2)(e)
>
> When a business collects consumers' personal information offline, it may, for example, include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice ***prior to collection***, or post prominent signage ***describing in***

detail the information specified in section 999.305(a)(1), which may also direct consumers to **a** ~~the~~ web ***page with further information on the notice*** ~~where the notice can be found~~.

We propose the following language in Section 999.305(b)(3):

If the business sells personal information, the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" required by section 999.315(a), or in the case of offline notices, ***prominent signage describing in detail the information specified in 999.305(a)(1), which may also direct*** consumers to ***a web page with further information on the notice*** ~~the web address~~ ~~for the webpage to which it links~~ .

We propose the following language in Section 999.306(b)(2):

"A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods include~~, but are not limited to,~~ printing the notice on paper forms that collect personal information, providing the consumer with a paper version of the notice ***prior to collection***, and posting ***prominent*** signage ***describing in detail the information specified in 999.305(a)(1),*** ~~directing~~ ***which may also direct*** consumers to a ***web*** page containing ***further information on*** the notice."

2. Opt-Out Through Global Setting: Section 999.315(a) allows consumers to opt-out of the sale of their personal information through a minimum of two or more methods, including a browser plugin or privacy setting as specified in 1798.135(c) and further defined in 1798.185(a)(4)[1], but the regulation should clarify that this includes a *global* device or browser setting. This is an incredibly important component of the law and critical to its function in the marketplace. Businesses should not be able to preclude consumers from exercising their right to opt-out through a global setting, as authorized by Civil Code section 1798.135(c), by limiting consumers to two, less convenient, opt-out methods.

We propose amending Section 999.315(a) as follows:

"…a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as: a browser plugin or privacy setting, ***global device setting*** or other mechanism, that communicate…"

[1] Section 1798.135(c) permits a consumer to authorize a person to opt-out of the sale of the consumer's personal information on the consumer's behalf. Section 1798.140(n) defines person broadly to include "an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert." For example, a browser, device setting, or User Agent would be considered a person for purposes of a consumer's exercise of the right to opt-out.

We propose amending Section 999.315(c) as follows:

"If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as: a browser plugin or privacy setting, ***global device setting*** or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 ***and Civil Code section 1798.135(c)*** for that browser or device, or, if known, for the consumer."

Finally, with respect to this concept, we propose amending Section 999.315(g) as follows:

"...User-enabled privacy controls, such as: a browser plugin or privacy setting, ***global device 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."

In addition, section 999.306(c)(2) should clarify that the business must provide notice of the "methods" by which the consumer may opt-out, not simply a "webform":

(2) The ~~webform~~ ***methods*** by which the consumer can submit their request to opt-out online, as required by Section 999.315(a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out;

~~(3) Instructions for any other method by which the consumer may submit their request to opt-out;~~

The guidance surrounding the privacy setting or global device setting should ensure that it is:

(i) ***consumer-friendly, clearly described, and easy to use by an average consumer, and does not require that the consumer provide additional information beyond what is necessary***; ***(ii) clearly represent a consumer's intent and be free of defaults constraining or presupposing such intent; (iii) ensure that the global opt-out preference signal does not conflict with other commonly-used privacy settings or tools that consumers may employ; (iv) provide a mechanism for the consumer to selectively consent to a business's sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting their preferences with respect to other businesses or disabling the opt-out preference signal globally.***

Finally, the Attorney General should consider certifying existing privacy or device settings, such as the **Do Not Track preference expression as defined by the W3C**[2], as adequate for the purpose of indicating a consumer's intent to opt-out of sale of the consumer's personal information. This would ensure that a global setting is available to consumers when the law goes into effect in 2020..

3. Opt-Out Button or Logo: Section 999.306(e) proposes to clarify the scope of the use of an opt-out button or logo in future regulations. We strongly recommend that the future regulation require that the button or logo indicate at a glance the consumer's opt-out state, such as by graying-out the button or logo or changing its appearance when the consumer has exercised the right to opt-out. Consumers should be able to ascertain their opt-out status immediately upon visiting a website or service with very low effort.

4. Obligations of Business that has Received Opt-Out Request: In some cases, such as where a consumer has cleared cookies or where browser technology makes it difficult for a business to identify repeat visitors, a business may not be able to identify whether a consumer has exercised the right to opt-out. This challenge could be addressed in part by requiring the opt-out button or logo to indicate the consumer's opt-out state and by technology, such as a global setting that allows the consumer to convey the consumer's intent to opt-out on each visit to a website. We propose adding subdivision (f) to Section 999.306 to read as follows:

(f) A business that receives an opt-out request from a consumer or the consumer's authorized agent, shall refrain from:
(a) Selling the consumer's personal information; and
(b) Asking the consumer to opt-in to the sale of their information, for 12 months from the date of receipt of the consumer's last opt-out request.

5. Immediate Implementation of Opt-Out Request: Section 999.315(d) gives businesses a 15-day grace period after receipt of a consumer's opt-out request before the business must stop selling the consumer's personal information. Although the CCPA provides businesses with a 45-day period to respond to requests for information and deletion, there is no corollary for the right to opt-out, which was intended to take effect immediately. While we understand that it may take a short period of time for a business to implement a consumer's opt-out request, the burden should be on the business to stop selling the consumer's personal information *immediately* upon receipt of the consumer's opt-out request unless the business can demonstrate that it is not technically feasible to do so, and in no event should a business be permitted to continue selling the consumer's personal information more than after 24 hours after receipt of the consumer's opt-out request.

[2] https://www.w3.org/TR/tracking-dnt/

In addition, section 999.315(f) requires a business to notify third parties with whom it has shared the consumer's personal information within 90 days of the business's receipt of the consumer's opt-out request to instruct those third parties that they may no longer sell the consumer's personal information. While we appreciate the Attorney General's effort to extend the consumer's opt-out request to third parties, we are concerned that this will create confusion. Indeed, some have already suggested that this regulation would allow businesses to continue to sell information older than 90 days, a position that has no support in the text of the CCPA. For the sake of simplicity and practicality, we suggest a simple rule: as soon as a consumer requests a business to stop selling their personal information, all that consumer's personal information in the possession of the business is "frozen" with respect to future sales.

6. Access to Highly Sensitive Information: Section 999.313(c)(4) imposes an absolute bar on consumers' access to certain highly sensitive information (e.g., social security number, health insurance number, etc.) While we recognize that more care must be taken with respect to requests for certain highly sensitive information, rather than banning consumers' access to such information completely, the regulations should allow businesses to impose higher standards for the verification of requests for access to highly sensitive information. Banks, credit card companies and hospitals/medical testing centers give consumers their information today, for example, and the technology exists to do so safely. We are concerned there will be a decrease in the impact of the law if consumers can't access ***all*** their personal information.

7. Expansion of Service Provider Exception to Include Service Providers to Government Agencies: Section 999.314 expands the definition of "service provider" to include a person or entity that provides services to a person or organization that is not a business. Although the CCPA does not directly regulate government agencies, it clearly limits the exception for "service providers" to entities that provide services to "businesses." Therefore, an organization that qualifies as a "business" under the CCPA should not escape the reach of the CCPA when it processes information on behalf of a government agency, and like other businesses, should be required to comply with consumer requests under the CCPA. There is no statutory basis for the wholesale exemption created in this regulation, and it is inconsistent with the intent of the law, which is to enable consumers to learn what information businesses have collected about them, regardless of the source.

8. Civil Code Section 1798.140(w)(2): It is not clear whether Section 999.314(b) is intended to include entities identified by Civil Code section 1798.140(w)(2) (referred to a "contractors" for purposes of this comment).

Since the Legislature enacted CCPA with distinctions between persons defined by Civil Code section 1798.140(w)(2) and service providers, we assume that Section 999.314(b) is not an attempt to combine the two because a person cannot be a contractor and service provider simultaneously. We therefore suggest the following language for clarification:

"To the extent a business directs a person or entity to collect personal information directly from a consumer on the business's behalf, and ***that person or entity is not a person defined by Civil Code section 1798.140(w)(2) and*** would otherwise meet all other requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations."

10. Combining of Information: Section 999.314(c) restricts service providers from combining 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. We support the Attorney General's efforts to require the siloing of information by service providers. We suggest clarifying that when an entity receives personal information in its capacity as a "service provider" it cannot use that information as a "business" on its own behalf.

11. Service Providers and Requests for Access and Deletion: Section 999.314(d) requires service providers to comply with consumer access and deletion requests. It is not clear whether this regulation is intended to permit a service provider to deny an access or deletion request on the grounds that the service provider only has information about the consumer in its role as a service provider and that the request should be directed to the business. We think that CCPA, as written, ***requires*** that service providers that qualify as businesses, ***must*** comply with access and deletion requests.

12. Definition of Financial Incentive: Section 999.301(g) defines the term "financial incentive" as follows:

"Financial incentive" means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information.

We propose modifying the definition as follows:

"Financial incentive" means a program, benefit, or other offering, including payments to consumers as compensation, for the ***collection,*** disclosure, ~~deletion~~ ***retention***, or sale of personal information.

We propose including the term "collection" to ensure consistency with Civil Code section 1798.125(b)(1), which allows a business to offer a financial incentive to consumers, under specified conditions, for "the collection of personal information . . ." Because of the term's broad definition in CCPA, we think it makes sense to include it here.

We also propose replacing "deletion" with "retention" to accurately reflect the intent of the law, which is to prohibit businesses from penalizing consumers for exercising their rights under the CCPA, including the right to deletion, while authorizing businesses to offer financial incentives to consumers who do not exercise those rights, e.g., a business may charge a consumer who allows a business to sell the consumer's personal information less than a consumer who opts-out of the sale of the consumer's personal information, provided other conditions are satisfied. Thus, the law was intended to allow a business to charge a consumer who allowed the business to retain the consumer's personal information less than a consumer who requested that the business delete the consumer's personal information, provided that other conditions are satisfied.

Note that with respect to a consumer who opts-out of the sale of the consumer's personal information, the business may continue to use that information as permitted by the CCPA, and therefore the financial incentive should be limited only to the value of the sale of the consumer's personal information and not to other rights, such as the consumer's right to delete the consumer's personal information.

13. Definition of "Typical consumer": Section 999.301(s) defines the term "typical consumer" to mean "a natural person living in the United States." We suggest amending the definition to refer to the "average" American consumer of that particular business. Without this clarification, businesses will be able to cherry-pick which of their consumers to use to justify their calculations. Given that some consumers are less profitable than others, allowing businesses to select only those consumers for purposes of calculating the value of consumer data would undermine the intent of the law.

14. Availability of Multiple Languages in Notice: Section 999.305(a)(2)(c) requires that notices be available in languages in which the business interacts with consumers in the ordinary course. To ensure that the primary notice is not obscured by a notice that is printed in multiple languages, the regulation should be clarified to require the business to provide notice to the consumer in the language that the business regularly uses to interact with the consumer, or in the predominant languages spoken in California, provided that consumers can easily access notices in other languages that are not displayed.

15. Definition of Explicit Consent: Section 999.305(a)(3) requires businesses to obtain "explicit consent" from consumers for the use of the consumers' personal information for a purpose not previously disclosed. However, the regulation does not define "explicit consent." We propose that the regulations define "explicit consent" to ensure that businesses do not treat notice of a change in the terms of their privacy policy as "explicit consent" for a new use of consumers' personal information. We propose the following definition:

"Explicit consent" means any freely given, specific, informed and unambiguous indication of the consumer's wishes by which the consumer, the consumer's legal guardian, or a person who has power of attorney or is acting as a conservator for the consumer, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose, such as by a statement or by a clear affirmative action. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute explicit consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute explicit consent. Likewise, agreement obtained through use of dark patterns does not constitute explicit consent.

16. Definition of "Categories of third parties" and Notice Requirements Applicable to Businesses that Collect Information Indirectly: Section 999.301(e) defines "categories of third parties" to mean entities that do not collect personal information "directly" from consumers. The regulations should, consistent with the intent of the CCPA, be re-oriented based on consumer-expectations, rather than the means by which the business collects the information. For example, an advertising network may be collecting information directly from a consumer's browser even though the consumer has no idea this is occurring. Similarly, a consumer who visits the New York Times website may not realize that a Facebook pixel on the page is collecting the consumer's personal information. To address this disconnect, we recommend that the regulations distinguish between businesses with which the consumer intentionally interacts, and those that collect the consumer's personal information even though the consumer is not intentionally interacting with them.

We propose the following modification to 999.301(e):

""Categories of third parties" means entities that collect personal information from consumers, with whom the consumer is not intentionally interacting, including but not limited to advertising networks, data analytics providers, government entities, social networks, and consumer data resellers."

We propose the following definition of "intentionally interacts":

"Intentionally interacts" means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, such as visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person."

17. Notice of Right to Opt-Out: Section 999.306(b)(1) sets forth the notice requirements for the right to opt-out. Most consumers do not read the information on the landing page. Therefore, we propose the following clarification to the regulation:

A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website homepage or ~~the download or landing page of a mobile application~~ ***with respect to a mobile application or online service, a standalone notice prior to downloading, installing, or activating the application or service, as well as an easily available link within the application or service***. The notice shall include the information specified in subsection (c) or link to the section of the business's privacy policy that contains the same information.

18. Privacy Policy: Section 999.308(a)(3) sets forth the requirements for privacy policies. In order to clarify that privacy policies are readily available to consumers at all times, we recommend modifying paragraph (3) as follows:

The privacy policy shall be posted online through a conspicuous link using the word "privacy," on the business's website homepage or on the download or landing page of a mobile application ***as well as an easily available link within the application or service***. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers.

19. Methods for Submitting Requests to Know and Delete: Section 999.312(e) describes the requirements applicable to businesses that do not "interact directly" with consumers. We are uncertain what this phrase adds, and would propose to modify the language to read: ~~If a business does not interact directly with consumers in its ordinary course of business, a~~ **At** least one method by which a consumer may submit requests to know or requests to delete shall be online, such as through the business's website or a link posted on the business's website.

20. Response to Requests to Delete: Section 999.312(d)(3) allow a business to delay its deletion of a consumer's personal information stored on a backup system until that system is next accessed or used. We agree with this approach but the regulation should make clear that the information may not be used for any purpose pending its deletion:

If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is next accessed or used***,***

provided that the business may not the personal information for any purpose pending its deletion.

In addition, the regulation should ensure that businesses do not present information to consumers regarding the right to delete that is designed to coerce consumers into refraining from exercising that right or in a manner that makes it difficult for a consumer to exercise the right to delete.

We propose the following amendment to Section 999.313(d)(7):

In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered, and more prominently presented than the other choices, **and the choice is not designed to coerce consumers into deleting only a portion of their information.**

We propose adding paragraph (8) to subdivision (d) of Section 999.313:

"A business may respond to a request to delete by describing in clear terms what will happen if a consumer's information is deleted, provided that the business shall not present the information in a manner designed to coerce consumers into refraining from deleting the consumer's personal information or in a manner that makes it difficult for the consumer to exercise the right to delete."

21. Requests to Opt-In After Opt-Out: Section 999.316 addresses a consumer's right to opt-in after opting-out. We recommend clarifying subdivision (b) as follows:

"A business may inform a consumer who has opted-out when a transaction requires the sale of their personal information as a condition of completing the transaction, ***why such transaction requires the sale of their information, and what parts of it must be sold,*** along with instructions on how the consumer can opt-in ***to its sale***."

22. Rights of Household: Section 999.318 addresses the rights of household to submit access and deletion requests. We recommend that the regulation also address the right of a household to opt-out of the sale of personal information, such as a shared television or device.

23. Discriminatory Practices: Section 999.336(c)(2) provides illustrative examples regarding financial incentives. We recommend adding the following additional example:

if a retailer offers a loyalty card program to its shoppers, it must allow the consumer to opt-out of the sale of the consumer's information, and may only charge a fee for such opt-out if the fee is reasonably related to the value the retailer obtains from selling the consumer's information, which the retailed collected as a result of monitoring the consumer's purchases as part of the loyalty program.

24. Support of Regulations: In addition to the previous suggestions, here are sections of the Regulations we had no comments upon, but we are supportive of:

- **§ 999.305(a)(2)(e):** We strongly support the requirement that the notice at collection be visible **before** any personal information is collected, and that it is clearly visible.
- **§ 999.305(a)(4):** We support the requirement that a new actual notice be provided prior to collecting additional categories of information.
- **§ 999.305(d):** We support this section, it is essential that consumers get control over the vast amount of their information being sold by companies they've never heard of, this section will help achieve this goal.
- **§ 999.306(b)(2):** It is absolutely critical that offline activities be covered, that is CCPA's intention and we are pleased to see this language around offline notices.
- **§ 999.307:** This section is clear and well thought-out. We think it will provide clarity, and empower consumers to make informed decisions.
- **§ 999.307(a)(2)(e):** Good, vital to have the financial incentive notice available **before** the consumer opts in.
- **§ 999.308(b):** This section was very clear and concise. These rights are the core of CCPA, and having them presented clearly is important.
- **§ 999.313(c)(5):** We support the concept that businesses must explain why they are denying a request to know.
- **§ 999.313(c)(9):** We support this concept strongly as we believe it will incent businesses to have one set of practices for all consumers, which can be more easily monitored and will be privacy-protective for consumers.
- **§ 999.313(d)(1):** We think the idea of defaulting to an opt-out if a deletion request is not honored, is a good one.
- **§ 999.313(d)(4):** We like the idea of specifying how a business has deleted the information.
- **§ 999.313(d)(6)):** We appreciate the transparency of this entire clause.

- **<u>§ 999.315(c)</u>:** The ability of a consumer to opt-out using a browser or device setting is central to the law, and was always part of the framework of CCPA. 1798.135(c) has always provided for this, and we are glad to see this in the regulations.

Thank you for your consideration of our comments.

Yours sincerely,

/s/ Alastair Mactaggart, Chair

Californians for Consumer Privacy

Message

From: Adrine Adjemian [redacted]
Sent: 12/4/2019 11:14:10 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA - Notice at the Point of Collection to Employees

Hi,

We are employee benefits attorneys based out of San Francisco and we represent single employers who are subject to the California Consumer Protection Act. It is our understanding from Assembly Bill 25 which amended the Act that the collection of personal information of employees is not subject to the Act until January 1, 2021 except for the Notice at the Point of Collection and the Private Right of Action provisions.

We are struggling with how we should be advising our clients regarding the Notice at the Point of Collection because the Proposed Regulations provide that a link to the business's privacy policy should be included in that Notice and the Proposed Regulations also set forth what should be contained in the Privacy Policy. However, if employers are required only to provide the Notice at the Point of Collection to employees in 2020 and not to comply with the other Privacy Policy requirements, does the Notice at the Point of Collection still need to contain a link to the Privacy Policy? We note that privacy policies are generally geared toward consumers and not employees and while we may need to advise our clients to prepare privacy policies specifically for employees next year, we are not sure if providing a link to the general Privacy Policy in the Notice at the Point of Collection to employees will suffice for 2020.

Any guidance is much appreciated!

Best,

Adrine

Adrine Adjemian | Associate | **Trucker Huss, APC**
ERISA and Employee Benefits Attorneys
One Embarcadero Center, 12th Floor | San Francisco, CA 94111-3617
[redacted] | www.truckerhuss.com | Download vCard

Message

From:	Valenzuela, Lauren [redacted]
Sent:	12/7/2019 12:57:58 AM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject:	CCPA Comment
Attachments:	CCPA Comment on Regulations 12.6.2019.pdf

Please see the comment attached.

LAUREN VALENZUELA, ESQ.
Corporate Counsel

[redacted]

PERFORMANT

PERFORMANT

Sent Via Email:
PrivacyRegulations@doj.ca.gov

CA Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St., First Floor
Los Angeles, CA 90013

December 6, 2019

RE: California Consumer Privacy Act (CCPA) Proposed Regulations

Dear Mr. Becerra:

We appreciate the opportunity to comment on the proposed CCPA regulations. As the employer of many California residents, and as a financial service company[1] who has designed its processes around protecting consumers privacy, we support a law which expands consumer privacy rights in California. Nonetheless, it has been our observation that many financial service companies, such as banks, credit unions, lenders, collection agencies and the like are having a difficult time operationalizing this law since the CCPA seems to have been designed for businesses who primarily operate and interact with consumers online or through applications (such as Facebook, Google, Lyft, Amazon, etc.) On its face, the GLBA exception seems like it would apply to many financial service companies, but there are many instances where our data collection does not squarely fit within the GLBA exception. This creates much uncertainty when trying to adapt the CCPA. We were hoping that the proposed regulations would have provided more guidance for companies who are not internet-based companies, however, we did not find that the proposed rules provided much clarity. We hope that our comments assist the AG promulgate rules which will help companies who are not AdTech or internet-based companies comply with the CCPA.

Notice at Collection of Personal Information
Section 999.305(a)(2) of the proposed rules states that the notice should be "designed and presented to the consumer in a way that is *easy to read and understand* to an average

[1] One of Performant's main lines of business is collecting debt. Performant has been providing this financial service to many federal, state, and private entities since 1976. One of the main federal laws governing debt collection is the Fair Debt Collection Practices Act (FDCPA), codified at 15 USC §1692 *et seq*. California has its own debt collection law as well, the California Rosenthal Act, codified at California Civil Code § 1788 et seq. Protecting and honoring a consumer's privacy is a core tenant of these laws, and for many years law-abiding debt collectors, such as Performant, have designed their debt collection processes around protecting a consumer's privacy.

consumer." This presupposes that the notice will be in writing. What if the notice is not provided in writing? What if there is nothing seen nor sent to the consumer because the information is being collected during a telephone conversation; may the notice be provided verbally in this kind of situation? We suggest that the rules speak to the situation where the information is being collected verbally. We have included suggested language in Exhibit A.

Similar to the above, § 999.305(b)(1) and §999.305(c) speak to the notice being provided in writing/being provided online. Not all means of data collection are done online, as it is common to collect information over the telephone. Accordingly, the proposed rules need to provide guidance when the notice is provided verbally.

We note, however, that if personal information is being collected over the telephone, it may be laborious for consumers to sit through a verbal disclosure of such a notice. Frequently, consumers become impatient and annoyed when they are required to listen to long disclosures of information. Accordingly, and in the alternative, we recommend that if the data collection is done verbally over the telephone, that the AG promulgate a rule that states that a business is only required to notify the consumer of where they may find the disclosure in writing (e.g., website) or be offered to have such written notice mailed or emailed to him/her. In order to avoid creating a negative consumer experience, and as a matter of practicality and convenience for consumers, we believe this would be permitted under the statute since consumers would still have access to this information. Another option is to allow businesses to provide an abbreviated notice verbally, which would include reference to where a consumer may find the full notice at his/her convenience (such as on a webpage or perhaps provide the consumer with the option to have the full notice mailed or emailed to him/her).

Service Providers
Section 999.314(a) of the proposed rule states: "To the extent that a person or entity provides services to a person or organization that is *not a business*, and *would otherwise* meet the requirements of a 'service provider' under Civil Code section 1798.140(v), that person or entity *shall be deemed a service provider* for purposes of the CCPA and these regulations." This proposed regulation creates much confusion. For example, Performant has state and federal governmental clients (who are nonprofits under the statute). If those non-profit governmental clients are not subject to the CCPA, why should Performant, as its service provider, still be required to respond to deletion and data requests received for personal information/data collected on behalf of our non-profit state and federal governmental clients? It also raises the following questions:

1. If a service provider has non-profit client who is exempt from the CCPA, and that service provider is collecting information for that non-profit client, must that service provider provide notice at or before the time of collection (since their non-business client did not provide such notice)? Note, the statute is clear that a business, not a service provider, must provide the notice (Cal. Civ. Code §1798.100(b)). Accordingly, if it is the AG's position that in this situation a service provider is required to provide notice, the regulations should explicitly state so.

2. If a service provider has a non-profit client who is exempt from CCPA, does that mean a service provider must provide channels for the consumer to make deletion requests and requests for information? Note, the statute is clear that a business, not a service provider, must provide such channels (Cal. Civ. Code §1798.130(a)). Accordingly, if it is

the AG's position that in this situation a service provider is required to provide channels for consumers to make such requests, the regulations should explicitly state so.

If the answer to both of the questions above is yes, that a service provider must provide notice and provide channels for consumers to make such requests when its clients are not businesses as defined by the statute, it seems that such a rule would run contrary to the statute which only requires these things of businesses (not service providers). Therefore, we recommend removing proposed rule in § 999.314(a) altogether and replacing it with a proposed rule that clarifies that if a service provider's client is exempt from the CCPA, so is the service provider (see the proposed language contained in Exhibit A). This would eliminate the confusion created over whether the requirements set forth in §1798.100(b) and §1798.130(a) flow down to service providers.

Additionally, we encourage the AG to think further about the requirement that service providers are required to supply information when they receive a request for information. The reason for this is because the service provider may not own the information they have in their possession, and/or may not be in a position to know what may or may not be supplied. For example, many service providers simply store data for businesses (e.g., a cloud-based customer relationship management (CRM) system). If a service provider receives a request for information, it is more logical for the service provider to instruct the consumer on where to direct that request to (i.e., its client/the business), and to provide contact information for that business, rather than respond to the request with specific information.

Sharing Information with Licensed Professionals (e.g., Attorneys, CPAs, etc.)
A company may share a consumer's personal information with its outside legal counsel in order for that legal counsel, for example, to defend the company against a suit brought by a consumer. Is this kind of information exchange subject to the CCPA, wherein a company would need to have the law firm sign and agree not to sell personal information so that it is treated as a service provider, and not a third party, under the CCPA? Outside legal counsels are bound by the Rules of Professional Conduct. Outside legal counsels do not "sell" consumer information they receive from their clients, as this would be contrary to the rules governing lawyers. In a similar vein, is information exchanged with other professionals, such as external auditors, CPAs, and tax firms, subject to the CCPA? It would be helpful for the AG to provide clarity on this matter.

Once again, thank you for the opportunity to comment. We hope that the final rules provide guidance for the financial services industry so that we may confidently comply with the CCPA and uphold consumers rights to fullest extent possible. Should you or your staff need a knowledge resource in the ARM industry, please know that Performant would welcome any opportunity to assist you and your staff in this manner.

Sincerely,
Lauren Valenzuela
Lauren Valenzuela, Esq.
Corporate Counsel
[redacted]

Exhibit A – Suggested Edits to the Proposed Regulations

§ 999.305 Notice at Collection of Personal Information

(a) Purpose and General Principles

1) The purpose of the notice at collection is to inform consumers at or before the time of collection of a consumer's personal information of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used.

2) The notice at collection shall be designed and presented to the consumer in a way that is easy to ~~read and~~ understandable to an average consumer. The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

~~a.~~b. Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.

c. If the notice is provided in writing, it shall:

~~b.~~d. Be easy to read and ~~U~~use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

~~c.~~e. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.

~~d.~~f. ~~Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.~~

g. Be visible or accessible where consumers will see it before any personal information is collected. For example, when a business collects consumers' personal information online, it may conspicuously post a link to the notice on the business's website homepage or the mobile application's download page, or on all webpages where personal information is collected. When a business collects consumers' personal information offline, it may, for example, include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to the web address where the notice can be found.

3) If the notice is verbal, it shall:

a. Be spoken in a clear and articulate manner.

~~e.~~b. Inform the consumer where the notice may be found in writing, such as on a webpage, or inform the consumer that the notice may be mailed or emailed to the consumer at their request.

§ 999.314(a)

To the extent that a person or entity provides services to a person or organization that is not a business~~, and would otherwise meet the requirements of a 'service provider' under Civil Code section 1798.140(v),~~ that person or entity shall not be deemed a service provider for purposes of the CCPA and these regulations.

Message

From:	Gary LaFever [redacted]
Sent:	12/6/2019 10:26:25 PM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject:	CCPA Comment Letter
Attachments:	12-6-2019 Anonos CCPA Comment Letter.pdf

Via Email: PrivacyRegulations@doj.ca.gov

To: Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

The attached Comment Letter respectfully requests clarification of the requirements under the California Consumer Privacy Act ("CCPA" or "Act") for CCPA compliant de-Identification in order for companies to comply with their obligations under the Act.

Thank you in advance for your review and consideration of this request.

Best Regards,

- Gary

Gary LaFever
CEO, Co-Founder & General Counsel
Anonos

Enabling Lawful Repurposing & Sharing of Data

Gartner named Anonos as a "Cool Vendor" in Privacy Management.
Read the Report

Anonos

BigPrivacy Unlocks Data

December 6, 2019

Via Email: PrivacyRegulations@doj.ca.gov

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Request for Clarification of CCPA De-Identification Requirements

This Comment Letter respectfully requests clarification of the requirements under the California Consumer Privacy Act ("CCPA" or "Act") for CCPA compliant de-identification in order for companies to comply with their obligations under the Act.

- §999.313(d)(2)(b) – proposed CCPA regulation §999.313(d)(2)(b) provides that in the context of a company's obligations with respect to Responding to Requests to Know and Requests to Delete, a company may comply by "De-identifying the personal information."

- §999.323(e) – proposed CCPA regulation §999.323(e) provides that in the context of General Rules Regarding Verification, "If a business maintains consumer information that is de-identified, a business is not obligated to provide or delete this information in response to a consumer request or to reidentify individual data to verify a consumer request."

Given the importance of the proper interpretation of "de-identification" under the above enumerated proposed regulations, clarification of the requirements for de-Identification under the Act including, *inter alia*, clarification of issues raised in this Comment Letter with regard to differences between de-identification under CCPA and HIPAA, are respectfully requested so that companies can comply with §§999.313(d)(2)(b) and 999.323(e) of the proposed CCPA regulations.

The CCPA is an exemplary model of a forward-thinking data protection law that enhances privacy for individuals by providing incentives for companies to implement safeguards that proactively protect information *in advance of data misuse* by leveraging technically enforced risk-based controls over data *when in use* versus relying solely on (i) encryption of data when at rest or in transit (but not *when in use* and it is most vulnerable) and (ii) *after-the-fact* remedies that fail of their essential purpose to make aggrieved parties whole in the event of violations of their privacy.[1] In the CCPA, this incentive comes in the form of an exclusion from the definition of protected Personal Information, under §1798.140(o)(3) (as amended), of information that is de-identified in accordance with the Act's new heightened requirements for "de-Identification" under §1798.140(h). This incentive under the

[1] See https://www.ntia.doc.gov/files/ntia/publications/epic-ntia-nov2018.pdf

CCPA is analogous to incentives provided under the EU General Data Protection Regulation ("GDPR" or "Regulation") for "pseudonymising" data to provide proactive risk-based protection – *in advance* – against misuse of protected Personal Data under the Regulation.[2]

The importance of proactive risk-based technical measures to balance data innovation and protection of individual privacy rights in today's data driven world is highlighted by the fact that consent – *by itself* – is incapable of effectively protecting privacy rights.

> *"The free and informed consent that today's privacy regime imagines simply cannot be achieved. Collection and processing practices are too complicated. No company can reasonably tell a consumer what is really happening to his or her data. No consumer can reasonably understand it. And if companies can continue to have their way with user data as long as they tell users first, consumers will continue to accept the unacceptable: If they want to reap the benefits of these products, this is the price they will have to pay…But this is not a price consumers should have to pay. It is time for something new. Legislators must establish expectations of companies that go beyond advising consumers that they will be exploiting their personal information. For some data practices, this might call for wholesale prohibition. For all data practices, a more fundamental change is called for: Companies should be expected and required to act reasonably to prevent harm to their clients. They should exercise a duty of care. The burden no longer should rest with the user to avoid getting stepped on by a giant. Instead, the giants should have to watch where they're walking."*[3] (emphasis added)
>
> *"Maybe informed consent was practical two decades ago, but it is a fantasy today. In a constant stream of online interactions, especially on the small screens that now account for*

[2] The benefits of properly "Pseudonymised" data, as newly defined under Section 4(5) of the GDPR, are highlighted in multiple GDPR Articles, including:

- Article 6(4) as a safeguard to help ensure the compatibility of new data processing.
- Article 25(1) as a technical and organizational measure to help enforce data minimization principles and compliance with data protection by design and by default obligations.
- Articles 32, 33 and 34 as a security measure helping to make data breaches "unlikely to result in a risk to the rights and freedoms of natural persons" thereby reducing liability and notification obligations for data breaches.
- Article 89(1) as a safeguard in connection with processing for archiving purposes in the public interest; scientific or historical research purposes; or statistical purposes; moreover, the benefits of pseudonymization under this Article 89(1) also provide greater flexibility under:
    - Article 5(1)(b) with regard to purpose limitation;
    - Article 5(1)(e) with regard to storage limitation; and
    - Article 9(2)(j) with regard to overcoming the general prohibition on processing Article 9(1) special categories of personal data.
- In addition, properly Pseudonymised data is recognized in Article 29 Working Party Opinion 06/2014 as playing "a role with regard to the evaluation of the potential impact of the processing on the data subject…tipping the balance in favour of the controller" to help support Legitimate Interest processing as a legal basis under Article GDPR 6(1)(f). Benefits from processing personal data using Legitimate Interest as a legal basis under the GDPR include, without limitation:
    - Under Article 17(1)(c), if a data controller shows they "have overriding legitimate grounds for processing" supported by technical and organizational measures to satisfy the balancing of interest test, they have greater flexibility in complying with Right to be Forgotten requests.
    - Under Article 18(1)(d), a data controller has flexibility in complying with claims to restrict the processing of personal data if they can show they have technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the rights of the data subjects are protected.
    - Under Article 20(1), data controllers using Legitimate Interest processing are not subject to the right of portability, which applies only to consent-based processing.
    - Under Article 21(1), a data controller using Legitimate Interest processing may be able to show they have adequate technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the rights of the data subjects are protected; however, data subjects always have the right under Article 21(3) to not receive direct marketing outreach as a result of such processing.

[3] See https://www.washingtonpost.com/opinions/our-privacy-regime-is-broken-congress-needs-to-create-new-norms-for-a-digital-age/2019/01/04/c70b228c-0f9d-11e9-8938-5898adc28fa2_story.html

> *the majority of usage, it is unrealistic to read through privacy policies. And people simply don't…Moreover, individual choice becomes utterly meaningless as increasingly automated data collection leaves no opportunity for any real notice, much less individual consent. We don't get asked for consent to the terms of surveillance cameras on the streets or "beacons" in stores that pick up cell phone identifiers, and house guests aren't generally asked if they agree to homeowners' smart speakers picking up their speech. At best, a sign may be posted somewhere announcing that these devices are in place. As devices and sensors increasingly are deployed throughout the environments we pass through, some after-the-fact access and control can play a role, but old-fashioned notice and choice become impossible…Ultimately, the familiar approaches ask too much of individual consumers. As the President's Council of Advisers on Science and Technology Policy found in a 2014 report on big data, "the conceptual problem with notice and choice is that it fundamentally places the burden of privacy protection on the individual," resulting in an unequal bargain, "a kind of market failure."*[4] (emphasis added)

The fact that consent – *by itself* – is not up to the task of protecting the privacy rights of individuals highlights the critical importance of technical risk-based safeguards that protect data *when in use* like de-identifying data under the CCPA and pseudonymizing data under the GDPR. In fact, "the real promise of government intervention may lie in giving firms an incentive to use consumers' personal data only in reasonable ways."[5] And, if the only privacy-respectful alternative is to withdraw consent and to opt-out of having their data processed, this withholds from individuals the potential benefits of data processing and withholds from society as a whole the benefits of representative, non-discriminatory data analysis.[6]

For purposes of this Comment Letter, the heightened requirements for de-identification under the CCPA are referred to as "2020 De-ID Standards" to highlight a comparison between the modern requirements for de-identification under the CCPA and the standards for de-identification under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), referred to herein as "1996 De-ID Standards." The differences between 2020 De-ID Standards and 1996 De-ID Standards are not surprising since there is nearly a quarter of a century gap between the enactment of the two statutes and HIPAA was enacted prior to the popularity of widespread data sharing and combining whereas the CCPA was enacted in full awareness of these modern data processing practices.

The 2020 De-ID Standards under CCPA §1798.140(h) require that the following criteria must be met:

- The information "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular customer;" and
- The business must have implemented technical safeguards and business processes that prohibit re-identification; and
- The business must have implemented business processes to prevent inadvertent release even of the de-identified data; and
- The business must not make any attempt to re-identify the information.

The above makes clear that 2020 De-ID Standards require the existence of technical safeguards that prevent recipients of data from inadmissibly re-identifying individuals represented in a data set when the data is used on a widespread or "global basis." This "global de-identification" standard requires context-aware, risk-based management of re-identification risk. As a result, in the context of 2020 De-ID Standards, the potential re-identification risk that must be defended against "depends on what everyone else knows and can do with the dataset" because "re-identification can be highly accurate in cases where a

[4] https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/
[5] https://hbr.org/cover-story/2018/09/uninformed-consent
[6] https://slate.com/technology/2019/08/consent-facial-recognition-data-privacy-technology.html

supposedly de-identified dataset is analyzed using outside sources of information that are not, themselves, de-identified." [7]

The HIPAA 1996 De-ID Standard is described in the following quote:

> *The HIPAA Privacy Rule provides a standard for de-identification of PHI, which generally states that health information is not PHI if it does not identify an individual and there is no reasonable basis to believe that it can be used to identify an individual. The standard provides two methods—safe harbor and expert determination—by which health information can be designated as de-identified for purposes of the standard and thus used and disclosed outside the Privacy Rule's protections for PHI. Under both methods, de-identified data retains some risk of identification of the individuals (e.g., patients of a healthcare provider) who are the subject of the information.*
>
> *Neither method requires removal of identifiers of healthcare providers or others who serve the individuals who are the subject of de-identified information. Accordingly, HIPAA de-identified data may be de-identified with respect to patients, but may include names, national provider identifiers or other identifiers of healthcare providers or covered entity workforce members. CCPA does not except personal information about providers or workforce members from its definition of personal information, however.*[8] (emphasis added)

As noted above, neither the safe harbor nor the expert determination methods require de-identification of indirect identifiers that may be used to re-identify individuals represented in a data set. In 2012, the U.S. Health & Human Services Office for Civil Rights (OCR) stated in written guidance on HIPAA de-identification standards that "a covered entity's mere knowledge of [specific studies about methods to re-identify health information or use de-identified health information alone or in combination with other information to identify an individual] does not mean it has actual knowledgell that these methods would be used with the data it is disclosing. OCR does not expect a covered entity to presume such capacities of all potential recipients of de-identified data. This would not be consistent with the intent of the Safe Harbor method, which was to provide covered entities with a simple method to determine if the information is adequately de-identified."[9] Lastly, with respect to the popular safe harbor method of HIPAA de-identification, researchers in 2017 discovered a risk of unauthorized re-identification as high as 25-28% versus earlier studies that had reported risk of below .05%.[10] For the foregoing reasons, it is clear that HIPAA requires compliant data use only within locally controlled enclave or siloed environments – i.e., "local de-identification."

The difference between the de-identification standards under CCPA and HIPAA creates a significant risk to HIPAA covered entities, business associates and data aggregators that believe data sets de-identified using HIPAA 1996 De-ID Standards satisfy de-identification requirements under CCPA 2020 De-ID Standards since resulting data sets would include personal information about California consumers under the CCPA. If a business subject to the CCPA maintains HIPAA 1996 De-ID Standard de-identified data that does not meet CCPA 202 De-ID Standards, then the business would need to honor California consumers' rights under the CCPA and otherwise comply with the CCPA, including the right to opt-out of the "sale" of personal information and the right to request deletion of personal information, and may be required to register as a data broker with the California Attorney General as a condition to license or otherwise disclose the data for cash or other consideration.[11]

[7] See https://www.dwt.com/blogs/privacy--security-law-blog/2019/11/de-identified-data-under-the-ccpa

[8] See https://www.natlawreview.com/article/inconsistent-hipaa-and-ccpa-de-identification-standards-create-compliance-challenges

[9] See https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf at 28.

[10] See https://techscience.org/a/2017082801/

[11] https://www.natlawreview.com/article/inconsistent-hipaa-and-ccpa-de-identification-standards-create-compliance-challenges

For the foregoing reasons, we respectfully requested that the California Attorney General clarify the requirements for de-Identification under the CCPA including, *inter alia*, clarification of issues raised in this Comment Letter with regard to differences between de-identification under CCPA and HIPAA.

Respectfully Submitted,

Gary

M. Gary LaFever
CEO & General Counsel

Please email [redacted] with any questions.

Message

From: Peter Watson [redacted]
Sent: 12/7/2019 12:02:34 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: [redacted]
Subject: CCPA Comment Submission
Attachments: CSSA Comment Letter - CCPA Proposed Regulations.pdf

Dear California Attorney General:

The California Self Storage Association (CSSA) hereby submits the attached comments to the CCPA proposed regulations. Thank you for your consideration.

Sincerely,

Peter Watson
Sent on behalf of Ross Hutchings
Executive Director - California Selft Storage Association

This message is intended for the designated individual(s) or entity named and may contain confidential, privileged and/or proprietary information. If you are not the intended recipient, please notify the sender by reply email and delete immediately; any distribution or copy of this email is strictly prohibited.

CSSA
CALIFORNIA
SELF STORAGE ASSOCIATION

December 6, 2019

Via Email: PrivacyRegulations@doj.ca.gov

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Title 11, Law, Division 1, Attorney General, Chapter 20, California, Consumer Privacy Act Regulations, Proposed Text of Regulations.

To Whom It May Concern:

The California Self Storage Association ("CSSA")[1] appreciates the opportunity to comment on the implementing regulations for the *California Consumer Privacy Act of 2018* ("CCPA"). While supportive of the efforts of the California Attorney General ("CAG") to comply with the CCPA's directive, the CSSA has several recommendations to improve the regulations. The bolded, underlined text is taken from the proposal. The non-bolded text below is the CSSA's input on the particular provision. The CSSA requests that the CAG consider the comments, provide greater clarity to certain sections, and incorporate specific recommendations in the final regulations.

§ 999.301. Definitions

Proposed new definition/clarification to be included in the Regulations to address "IP Address Only Consumer Scenario".

Many CCSA members are small to medium sized private self-storage owners/operators that: (i) do not have annual gross revenues in excess of $25,000,000; (ii) do not derive 50 percent of more of their annual revenues from selling consumer's personal information and (iii) are uncertain as to whether or not they buy, receive or sell the personal information of 50,000 or more consumers, households or devises.

The reason for the uncertainty surrounding item number (iii) above is that, many of these companies have less than 50,000 customers/tenants or prospective customers/tenants (a metric that is easily identifiable), but may receive 50,000 or more non-customer visitors to their websites, and presumably, these websites cache the consumers' IP Address immediately upon the consumers visitation to the website even if the consumer is a mere browser that does not engage any services or provide any other information while visiting the website.

This scenario was outlined by Mr. Watson, a CSSA Board Member, during the public comments

[1] CSSA is a California state trade association predominately comprised of self storage owners, operators/managers and venders.

in Los Angeles on December 3, 2019 (speaker No. 11), and referred to by Mr. Watson as the "IP Address Only Scenario." These companies desire to know whether or not the CCPA applies to their business, but there are technological challenges that render such determination extremely difficult (if not impossible). Namely, the companies are technologically challenged in (1) determining how many California IP Addresses visit the business' website (as opposed to out of state consumers); and (2) determining how many of those California IP Addresses are non-existing tenant/customer or non-potential tenant/customer that are already counted towards the 50,000 threshold.

Simply stated, as currently drafted, there will be a vast number of business that do not know whether they are subject to the CCPA, and requiring these companies implement significant privacy policies and procedures to comply with the CCPA when they might not be subject to same, will likely cause confusion to both the consumers and the businesses.

Under this context, the CSSA respectfully requests the implementation of one of the following proposed clarifications in the definition section of the regulations:

1. The first proposal, and preferred approach, would be to specifically exclude IP Addresses from the definition of "personal information" solely as it pertains to calculating the 50,000 consumer threshold. For the avoidance of doubt, this would not remove IP Addresses from the definition generally (only from the 50,000 threshold calculation). This proposal, if implemented, would eliminate the aforementioned IP Address Only Consumer Scenario, thereby providing clarity to both businesses and consumers of these businesses.

2. As an alternative to the first proposal, the AG could remove the consumer's right to request the deletion of personal information for businesses that would not qualify under the 50,000 consumer threshold but for the mere receipt of IP Addresses from website browsers. Under this second alternative, the consumer will still have the "right to know," via the business's privacy policy, however these businesses will no longer have the obligation to delete personal information upon a consumer's request.

"Household" means a person or group of people occupying a single dwelling.

The CSSA supports adding a definition for "household" as it is one of the threshold considerations for whether the CCPA is even applicable. However, the present definition is ambiguous. For example, what if a household is comprised of college students, two of whom are consumers under the statute and the third is a Colorado resident in California for school. The collection is no longer a group of "consumers" as the Colorado resident does not fit the definition. Does that mean that the entire group is no longer a "household"? If not, does that remove their ability to exercise rights under the CCPA? Conversely, does it remain a "household" and does the Colorado resident now possess new authority? privacy rights. Regardless, it should be clarified.

§ 999.305. Notice at Collection of Personal Information

(a)(2) Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.

The CSSA fully supports equal access to goods and services. In the context of compliance with the CCPA, it would be beneficial to both businesses and consumers if the CAG could provide more explicit guidance as to how a business can comply with the requirements of the statute to ensure consumers with disabilities are able to exercise their rights.

(a)(3) A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. 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 the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.

This section appears to place a greater compliance burden on a business if it subsequently determines it desires to use information in a manner not previously disclosed. As noted in (a)(1), "[t]he purpose of the notice at collection is to inform consumers at or before the time of collection of a consumer's personal information of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used." For a business that wishes to use personal information in a particular manner, the consumer is informed up front of that intent. However, if that same business later determines it wishes to use that same personal information, but in a different way, it must obtain "explicit consent" from the consumer. It appears that the CAG is placing a higher compliance burden on a business merely because of when and how it decided it wanted to use a consumer's personal information. From a policy perspective, it is not clear why additional requirements would attach to a determination that occurs after the initial notice is provided. The CSSA request that this provision be revised to make it consistent with the other notice provisions.

§ 999.308. Privacy Policy (b) The privacy policy shall include the following information: (5) Authorized Agent (a) Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf.

The CAG should provide further guidance to businesses as to how a consumer designates an authorized agent. Ideally a model form would be very helpful to clear uncertainty. The supplementary direction is essential so that companies may in turn provide additional guidance to consumers in their privacy policies. There is general uneasiness with third-party authorized agents attempting to exercise a California consumer's rights under the CCPA, as it seems ripe for scammers. First-party businesses need to fully understand how a consumer may designate an authorized agent. By extension, this will afford companies the understanding of the process to be able to fully explain it to California consumers.

Article 3. Business Practices for Handling Consumer Requests

§ 999.312. Methods for Submitting Requests to Know and Requests to Delete

(b) A business shall 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.

The two-step process is sensible to safeguard consumers' personal information; however, express limitations on the number of follow ups should be included in the final regulations. What is a business supposed to do if the consumer contacts the business and requests that it delete their personal information but then does not respond to the subsequent request to confirm their intent to delete? Must a business keep attempting to contact them? The final regulations should explicitly state that the business only must follow up one (1) time and if they do not respond within forty-five (45) days the request can be discarded. Businesses should not be required to endlessly follow up with consumers.

(c) A business shall consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. At least one method offered shall 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.

The CSSA understands the intent of this provision. However, a business should not be required to provide three (3) methods for a consumer to exercise their rights merely because it operates a traditional brick-and-mortar facility along with a web-based presence. In contrast, the CCPA only mandates two methods for a business that, for example, operates an e-commerce platform with no physical structure. The CAG should not penalize or reward a company merely because of its operational choices. CCPA-covered businesses should *all* be required to provide *two* methods as mandated by the statute. The CAG should not impose additional compliance obligations on businesses via these regulations simply because a business allows a consumer to interact with it both "online" and "in-person."

§ 999.313. (c)(6); § 999.323. (3)(d).

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

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

In the context of compliance with the CCPA, it would be beneficial to both businesses and consumers if the CAG could provide more explicit guidance as to what constitutes "reasonable security measures." Perhaps the CAG can adopt a set of standards that is available on this topic – the concern here is that business will not know how far to go to comply with the "reasonable security measures," and the lack of guidance could lead to confusion and unnecessary litigation.

§ 999.313. Responding to Requests to Know and Requests to Delete

(a) 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 information provided shall describe 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.

The additional requirement that businesses provide an initial notification to a consumer within ten (10) days of receipt is unnecessary and should be revised. Nothing in the CCPA mandates such an action and providing notice when a substantive response will be given does not provide additional value to the consumer. California businesses already will have to divert resources to respond to and comply with requests made under the CCPA. Adding extra requirements through these implementing regulations does not provide a substantive benefit to consumers, but rather a needless burden on business. While individual businesses may elect to provide an initial notification to consumers that the request has been received, they should not be required to do so.

If this 10 day notice is critical to effectuate the intent of the CCPA, the CSSA respectfully requests that the timing be extended to 10 business days, to avoid a technical violation due to holidays and weekends.

Responding to Requests to Know

(1) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).

(2) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall 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.

While the intent of the CCPA is to provide California consumers with greater control over their private information, there will inevitably be nefarious actors seeking to take advantage of the new law. As such, these provisions are essential to allow businesses to refuse a request to disclose categories or specific pieces of personal information if the company is unable to verify the identity of the individual making the request.

However, the provision that requires businesses to review the request as an inquiry for the categories of information if the request for specific information is denied is unduly onerous. If the business was unable to verify the identity of the requesting consumer for specific pieces of information, those issues are almost certainly going to remain for requests for the categories as well. The CSSA appreciates that the proposed regulations provides criteria to evaluate the request against the issue of improper disclosure, but concerns persist. The CSSA requests that the CAG remove the provision that requires that the business evaluate the request as one for the categories of personal information and instead allow the business to jump immediately to direct the consumer to its general collection practices. This will expedite and streamline the process for businesses and simultaneously safeguard consumer's personal information. Further still, consumers have an immediate remedy available to them should an issue manifest: he or she simply must provide the requested information and re-submit the request. Given the simple "fix" available to consumers, businesses should not be required to comply with the "step-down" approach outlined the regulations. This provision should be revised.

(5) If a business 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, the business shall inform the requestor and explain the basis for the denial. If the request is denied only in part, the business shall disclose the other information sought by the consumer.

The CSSA commends the CAG for providing greater clarity on how the exceptions to disclosure operate. However, additional guidance would be beneficial for businesses. The exceptions in the CCPA are worded broadly and additional guidance from the CAG would be helpful. For example, does the businesses' interpretation of the exceptions always "win"? If the business simply conveys that it will not comply with the request and identifies one or more exceptions without expanding further is that sufficient for the purposes of compliance? Does the consumer have the ability to contest that determination? If so, and if a conflict arises, whose interpretation carries the day? Regardless, it should be clarified further in the final regulations.

(d) Responding to Requests to Delete

(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.

CCPA-covered companies are concerned with individuals making false requests to delete information. Permitting businesses to deny the request if the identity of the requestor cannot be verified is sensible. However, the stepped-down approach that requires a business to treat that request as one to opt-out instead of a request to delete defies logic. If the threshold issue is the lack of verification of the requester's identity, why would a business deny that request to delete predicated upon that concern, but then presume that the request is valid and legitimate for the purposes of a request to opt-out? If a consumer does not appropriately verify their identity so that a business is reasonably certain that the request is from that individual, they should not be required to comply with the stepped down approach outlined in the proposed regulations. Instead, the business should be permitted to simply inform the consumer of the issue. This alternative approach is bolstered by the reality that consumers have an immediate means of redress: simply provide the requested information to confirm their identity. The CSSA requests that this provision be amended in the final regulations.

§ 999.317. Training; Record-Keeping

(a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall 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.

(b) A business shall maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.

(c) The records may be maintained in a ticket or log format provided that the ticket or log 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.

(d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

(e) 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.

The CAG is essentially dictating to businesses that it create additional information and data about consumers. Does this information have to be disclosed if a consumer makes a subsequent request under the CCPA? What if a consumer is aware of this recordkeeping requirement and makes a second request to delete that specifically identifies the recordkeeping component? Can the business use one of the safe harbor exceptions? This should be clarified in the final text.

Article 4. Verification of Requests

§ 999.323. General Rules Regarding Verification

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

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

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

(2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5(d), unless necessary for the purpose of verifying the consumer.

(3) Consider the following factors:

a. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5(d) shall be considered presumptively sensitive;

b. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;

c. The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;

d. Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;

e. The manner in which the business interacts with the consumer; and

f. Available technology for verification.

The CSSA applauds the CAG for providing the above-listed factors to assist businesses to confirm a consumer's identity. However, it would be helpful if the CAG further explained how the factors interact and yield a particular outcome. For example, should businesses treat the factors equally and employ a balancing approach? Additional clarification or guidance in this respect would be helpful.

§ 999.324. Verification for Password-Protected Accounts

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.

(b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to

delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer.

This section confirms businesses possess the authority to direct consumers, if they already have an account, to utilize it to confirm their identity. This is sensible and will provide businesses with an additional level of assurance that the purported consumer is truly that individual. In the alternative, it is helpful that the proposed regulation confirms that businesses that suspect fraudulent activity may elect to not proceed with the request and may request that the consumer follow additional verification steps to confirm their identity. The provision is sensible and should remain in the final text.

§ 999.325. Verification for Non-Accountholders

A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.

Mandating that consumers provide a signed declaration under the penalty of perjury is sensible, especially for requests to know specific pieces of personal information. In the wrong hands, that data can be devasting to a consumer's identity. While likely not perfect, the requirement that the signed declarations accompany the request along with three pieces of personal data will hopefully ensure that all requests are legitimate.

However, with that said, it seems probable that scammers will attempt to forge those declarations. It would be helpful if the CAG provided a template for those forms as part of the final regulations or somewhere on its website. Additional requirements, perhaps a mandate that the form be notarized, would provide an additional level of certainty to businesses that the request is legitimate while simultaneously safeguarding consumer's personal information.

§ 999.326. Authorized Agent

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, the business may require that the consumer: (1) Provide the authorized agent written permission to do so; and (2) Verify their own identity directly with the business.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent

with power of attorney pursuant to Probate Code sections 4000 to 4465.

(c) A business may deny a request from an agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

Businesses, including CSSA members, are wary of "authorized agents" exercising a third parties' rights under the CCPA. This area seems ripe for scammers and other nefarious actors to hold themselves out to businesses as "authorized" in order to obtain personal information or have it deleted. It is sensible to mandate that businesses confirm the identity of the consumer, even doing so directly when an authorized agent attempts to act on their behalf. However, if that is the threshold for confirmation absent a power of attorney, why permit authorized agents to act on the individual's behalf at all? Since the individual consumer must participate in the process anyway, why would an authorized agent be necessary? Direct requests from consumers should be required to eliminate confusion and confirm the intent of the individual.

Conclusion

The CSSA appreciates this opportunity to comment on the proposed regulations for the CCPA. Thank you for your thoughtful consideration of these comments.

Respectfully submitted,

Ross Hutchings

Ross Hutchings, CEA
Executive Director – California Self Storage Association

Message

From: CU Lawyers [redacted]
Sent: 12/6/2019 10:58:44 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Comments

The exclusion under Gramm Leach Bliley needs to include information collected by creditors in connection with the collection of an unpaid loan.

Please include this under the definition of the GLB exclusion.

Thank you

A. Lysa Simon

--
A. Lysa Simon
[redacted]

This communication, including any attachments, may contain information that is confidential and may be privileged and exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any use, disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender. Thank you for your cooperation. We are debt collectors.

Message

From: Christine Bannan [redacted]
Sent: 12/6/2019 9:41:02 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Marc Rotenberg [redacted]; Hunter Daley [redacted]; Caitriona Fitzgerald [redacted]
Subject: CCPA Comments
Attachments: EPIC-CCPA-Dec2019.pdf

Please find EPIC's comments attached.

Best Regards,

Christine Bannan

——————

Christine Bannan
EPIC Consumer Protection Counsel
Coordinator, Privacy Coalition
Electronic Privacy Information Center (EPIC)
[redacted]
privacycoalition.org

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

[redacted]
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CALIFORNIA OFFICE OF THE ATTORNEY GENERAL

NOTICE OF PROPOSED RULEMAKING

THE CALIFORNIA CONSUMER PRIVACY ACT

December 6, 2019

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the Notice of Proposed Rulemaking Action on the California Consumer Privacy Act ("CCPA").[1] EPIC thanks the Office of the Attorney General for its work on the proposed regulations and leadership on privacy issues.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has long supported the establishment of comprehensive federal privacy law and also argued that federal law should not preempt stronger state laws.[3] EPIC recently released *Grading on a Curve: Privacy Legislation in the 116th*

[1] California Department of Justice, Notice of Proposed Rulemaking Action, Title 11 (Oct. 11, 2019), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf.

[2] *About EPIC*, EPIC (2019), https://www.epic.org/epic/about.html.

[3] *See* Privacy in the Commercial World, H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection (testimony of Marc Rotenberg, Exec. Dir., EPIC) (March 1, 2001), https://epic.org/privacy/testimony_0301.html; *Hearing on the Discussion Draft of H.R.____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach*, H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade (testimony of Marc Rotenberg, Exec. Dir., EPIC) (June 15, 2011), https://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf; *Reauthorizing Brand USA and the U.S. SAFE WEB Act*, H. Comm. on Energy & Commerce, Subcomm. on Consumer Protection & Commerce (statement of EPIC) (Oct. 29, 2019), https://epic.org/testimony/congress/EPIC-HEC-SafeWebAct-Oct2019.pdf. *See, e.g.*, Video Privacy Protection Act of 1988, 18 U.S.C. 2710(f) ("The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.")

Congress.[4] EPIC's report sets out the key elements of a comprehensive federal privacy law: (1) strong definition of personal information; (2) establishment of an independent data protection agency; (3) individual rights; (4) strong data controller obligations; (5) algorithmic transparency; (6) data minimization and privacy innovation; (7) prohibits take-it-or-leave it and pay-for-privacy terms; (8) private right of action; (9) limits government access to personal data; and (10) does not preempt stronger state laws.

As the Attorney General considers ways to improve the text of the proposed California state regulations, EPIC submits these comments to evaluate how the proposal meets the framework criteria EPIC has proposed to the Congress.

Strong definition of personal information

EPIC commends the Attorney General's defense of a robust definition of personal information. The CCPA is the culmination of state-wide support from voters "to empower consumers to find out what information businesses were collecting on them and give them the choice to tell businesses to stop selling their personal information."[5] The California Legislature has "explained that an individual's ability to control the use and sale of their personal information was fundamental to the 'inalienable' right of privacy set forth in the California Constitution."[6] With these objectives in mind, the California Legislature has incorporated a strong definition of "personal information" into the Act.[7]

[4] *See* https://epic.org/GradingOnACurve/.

[5] CALIFORNIA SENATE JUDICIARY COMMITTEE, CALIFORNIA BILL ANALYSIS, S.B. 1121 Sen. (2018); *cf.* EPIC, *Public Opinion on Privacy*, https://epic.org/privacy/survey/.

[6] *California Department of Justice, Notice of Proposed Rulemaking Action*, at 9 (Oct. 11, 2019), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf.

[7] *See* Cal. Civ. Code §999.301; *reprinted in* Marc Rotenberg, THE PRIVACY LAW SOURCEBOOK 2020 (EPIC 2020).

The scope of a privacy bill is largely determined by the definition of "personal information." A good definition includes both data that is explicitly associated with a particular individual and also data from which it is possible to infer the identity of a particular individual. Personal information also includes all data about an individual, including information that may be publicly available, such as zip code, age, gender, and race.[8] All of these data elements are part of the consumer profiles companies create and provide the basis for decision-making about the individual. EPIC supports the California Legislature's broad definition of "personal information."

The AG should not modify the Act's strong definition of "personal information." The Act's definition of "personal information" is comprehensive and should not be modified. Furthermore, the AG should not endorse any proposed changes to the Act currently under consideration by the California Legislature, such as Assembly Bill 873 (AB-873).[9] Proposed changes to the Act in AB-873 add qualifying "reasonably" language to various definitions, including the definition of "personal information," which undermine the current definition in the Act and weakens data privacy protections for Californians.

Establishment of an Independent Data Protection Agency

Almost every democratic country in the world has an independent national data protection agency, with the competence, authority, and resources to help ensure the protection of personal data. These agencies act as an ombudsman for the public. Many now believe that the failure to establish a data protection agency in the U.S. has contributed to the growing incidents

[8] EPIC Comments to FCC, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 18-19 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002079241.pdf.
[9] *See* AB-873, Cal. Leg., 2019–20 Regular Sess. (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB873.

of data breach and identity theft.[10] EPIC has long supported the establishment of a federal data protection agency.[11]

A strong state privacy law would establish an independent state-level Data Protection Agency with resources, technical expertise, rulemaking authority and effective enforcement powers. EPIC commends the Attorney General's work on privacy issues, but recognizes that resource limitations and competing priorities of the office will make effective enforcement of California privacy rights difficult to do alone. An expert agency would be able to assist the AG with this critical responsibility. The California Privacy Rights and Enforcement Act of 2020 would establish a California Privacy Protection Agency that would assume rulemaking responsibilities, promote public awareness, provide guidance to consumers and businesses, provide technical assistance to the legislature, and cooperate with other agencies on consistent application of privacy protections.[12] EPIC recommends that the Attorney's General's office work in support of a California privacy agency.

Individual rights (right to access, control, delete)

Californians have strong individual rights under the Act, which EPIC supports.[13] Privacy legislation must give individuals meaningful control over their personal information held by others. This is accomplished by the creation of legal rights that individuals exercise against

[10] *Examining Legislative Proposals to Protect Consumer Data Privacy*, S. Comm. on Commerce, Sci., and Trans. (statement of EPIC) (Dec. 4, 2019); https://epic.org/testimony/congress/EPIC-SCOM-LegislativePrivacyProposals-Dec2019.pdf; *see also* EPIC, The U.S. Urgently Needs a Data Protection Agency, https://epic.org/dpa/.

[11] Marc Rotenberg, *In Support of a Data Protection Agency in the United States*, 8 Government Information Quarterly 79-93 (1991)

[12] Alastair Mactaggart, letter to Office of the Attorney General Initiative Coordinator re Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, and Request to Prepare Circulating Title and Summary (Amendment) Nov. 13, 2019, https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

[13] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev.

companies that choose to collect and use their personal data. These rights typically include the right to access and correct data, to limit its use, to ensure it is security protected, and also that it is deleted when no longer needed. These rights are present in the CCPA. "Notice and consent" has little to do with privacy protection. This mechanism allows companies to diminish the rights of consumers, and use personal data for purposes to benefit the company but not the individual. The proposed regulations maintain the individual rights granted to consumers in the Act, and EPIC supports the AG's decision to uphold them. Section 1798.100 of the Act grants the individual "right to know," Section 1798.130 grants the individual "right to access" and Section 1798.105 grants the individual "right to delete."[14]

Strong data controller obligations

Organizations that choose to collect and use personal data necessarily take on obligations for the collection and use of the data. These obligations help ensure fairness, accountability, and transparency in decisions about individuals. Together with the rights of individuals describes above, they are often described as "Fair Information Practices." Many of these obligations are found today in U.S. sectoral laws, national laws, and international conventions. These obligations include:

- Transparency about business practices
- Data collection limitations
- Use/disclosure limitations
- Data minimization and deletion
- Purpose specification
- Accountability
- Data accuracy
- Confidentiality/security

[14] Cal. Civ. Code §§ 1798.100, 105, 130.

The CCPA lacks several of these key provisions. For example, it lacks a presumption against disclosure, data security standards, and accountability mechanisms. The Legislature must update the CCPA to place responsibilities on companies.

Require Algorithmic Transparency

The California AG should require data brokers to identify the factors used in algorithmic decision-making practices. As automated decision-making has become more widespread, there is growing concern about the fairness, accountability, and transparency of algorithms.[15] All individuals should have the right to know the basis of an automated decision that concerns them. Modern day privacy legislation typically includes provisions for the transparency of algorithms to help promote auditing and accountability.[16]

Data broker registry requirements were incorporated into the Act in October 2019 in AB-1202. Under Cal. Civ. Code § 1798.99.82(b)(2)(B), data brokers are requires to provide "any additional information or explanation the data broker chooses to provide concerning its data collection practices."[17] EPIC supports this provision of the Act, but it is only the first step to transparency because it neither requires data brokers to provide information about the algorithms they use, nor the factors they incorporate into their data collection, management, and decision-making practices.[18] The AG should require data brokers to provide this information in order to

[15] *The Fair Housing Act: Reviewing Efforts to Eliminate Discrimination and Promote Opportunity in Housing*, H. Comm. on Financial Services (statement of EPIC) (Apr. 2, 2019), https://epic.org/testimony/congress/EPIC-HFS-FairHousingAct-Apr2019.pdf.

[16] EPIC, Algorithmic Transparency: End Secret Profiling, https://epic.org/algorithmic-transparency/; The Public Voice, *Universal Guidelines for Artificial Intelligence*, https://thepublicvoice.org/AI-universal-guidelines.

[17] Cal. Civ. Code § 1798.99.82(b)(2)(B).

[18] *See Universal Guidelines for Artificial Intelligence*, PUB. VOICE (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/; EPIC, *The Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html.

raise consumer awareness of how their personal data is being used and collected, as well as bring to light secret profiling systems which should be prohibited.

Data brokers that generate consumer scores must be required to reveal the factors that used to generate scores. There are many data brokers that generate "secret scores" about consumers which they track and sell to other companies.[19] These data brokers are "largely invisible to the public" and "most people have no inkling they even exist."[20] These companies make decisions that impact the ability of people to obtain jobs, credits, housing, and healthcare. Fortunately, these companies are covered by the Act and do not fall within the consumer reporting and financial institution exceptions.[21] Coverage must be preserved by the AG rulemaking.

Require Data Minimization and Privacy Innovation

Many U.S. privacy laws have provisions intended to minimize or eliminate the collection of personal data. Data minimization requirements reduce the risks to both consumers and businesses that could result from a data breach or cyber-attack.[22] Good privacy legislation should also promote privacy innovation, encouraging companies to adopt practices that provide useful services and minimize privacy risk. Privacy Enhancing Techniques ("PETs") seek to minimize the collection and use of personal data. The Legislature should consider adding data minimization requirements in a future update of the Act.[23]

[19] Kashmir Hill, *I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too* N.Y. Times (Nov. 5, 2019), https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html.
[20] *Id.*
[21] *See e.g., Can I use Sift for credit risk reporting?* SIFT, https://support.sift.com/hc/en-us/articles/202713053-Can-I-use-Sift-for-credit-risk-prediction- (last visited Dec. 5, 2019).
[22] EPIC Comments to Gov't of India, *White Paper of the Committee of Experts on a Data Protection Framework for India* 3 (Jan. 2018), https://epic.org/EPIC-IndiaDataProtection-Jan2018.pdf.
[23] *See* S. 1214, 116th Cong. § 12 (2019).

Prohibit take-it-or-leave-it or pay-for-privacy terms

Individuals should not be forced to trade basic privacy rights to obtain services. Such provisions undermine the purpose of privacy law: to ensure baseline protections for consumers.[24] Generally, the CCPA does not allow businesses to "discriminate against a consumer because the consumer exercised any of their . . . rights under [the Act]."[25] However, the Act allows businesses to offer pay-for-privacy "financial incentives" to consumers, so long as they are "reasonably related to the value provided to the consumer by the consumer's data."[26] EPIC opposes this pay-for-privacy exception in the Act, which is in violation of California's inalienable right to privacy, encourages consumer discrimination, and should be mitigated to the maximum extent available by the AG's rulemaking authority.[27]

The AG's proposed regulations require businesses to notify consumers of financial incentives in language "that is easy to read and understandable to an average customer."[28] Businesses that use financial incentives are also required to explain price or service differences to consumers.[29] Specifically they must provide "[a] good-faith estimate of the value of the consumer's data that forms the basis for" the financial incentive, and they must describe the method the business used to calculate the value of the consumer's data."[30] Short of an outright ban on pay-for-privacy, EPIC encourages the AG to consider additional language to strengthen

[24] *See* Marc Rotenberg, *Privacy Guidelines for the National Research and Education Network*, NCLIS (1992) ("Users should not be required to pay for routine privacy protection. Additional costs for privacy should only be imposed for extraordinary protection.") *reprinted in* Anita L. Allen & Marc Rotenberg, PRIVACY LAW AND SOCIETY 762 (2016); *see also* Marc Rotenberg, *Communications Privacy: Implications for Network Design*, 36 Communications of the ACM 61-68 (Aug. 1993).

[25] Cal. Civ. Code § 1798.125(a)(1).

[26] Cal. Civ. Code §§ 1798.125(a)(2), (b)(1).

[27] CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining . . . privacy.").

[28] Proposed Regs. § 999.307(a)(2).

[29] Proposed Regs. § 999.307(b)(5).

[30] Proposed Regs. § 999.307(b)(5).

the notice requirement in order to further deter businesses from harming consumers through excessive financial incentives.

Financial incentive calculation of the value of consumer data should be equal among all consumers. Most concerning in the proposed regulations are businesses ability to charge different prices based on consumer data.[31] The proposed regulations permit businesses to calculate the value of consumer data based on "separate tiers, categories or classes of consumers."[32] This is highly discriminatory and should be struck from the regulations. A recent report from the Australian Competition and Consumer Commission (ACCC) found that "[a] consequence of increasingly sophisticated data analytics and personalisation is that it may enable and encourage highly targeted price discrimination."[33] Specifically, businesses create highly detailed profiles on consumer "behaviours and attributes to offer each a different price for a product or service."[34] Allowing such categorization of consumers under the regulations have discriminatory effects against protected classes of Californians. For example, a recent University of California Berkeley study found that mortgage lenders profit 11.5% more on average from Latinx and African-American borrowers than other borrowers.[35]

Under the current proposed regulation, these businesses would be permitted to value Latinx and African-American consumer data higher than that other consumer classes, resulting in price discrimination. For households with limited financial resources, they may be left with no

[31] *See* Cal. Civ. Code § 1798.125.
[32] Proposed Regs. § 999.337(b)(3).
[33] Customer Loyalty Schemes, ACCC (Dec. 2019), https://www.accc.gov.au/system/files/Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF.
[34] Customer Loyalty Schemes, ACCC (Dec. 2019), https://www.accc.gov.au/system/files/Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF.
[35] https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf

alternative but to surrender to allowing businesses to use, share, and sell their personal data. To mitigate against these potential discriminatory practices, the AG should remove Section 999.337(b)(3) from the regulations and require businesses to calculate and apply data privacy financial incentives for all of its customers equally.

Private Right of Action

Privacy laws in the U.S. typically make clear the consequences of violating a privacy law. Statutory damages, sometimes called "liquidated" or "stipulated" damages are a key element of a privacy law and should provide a direct benefit to those whose privacy rights are violated.[36] The Legislature should consider expanding the Act's limited private right of action to include all violations of the Act. The Attorney General alone cannot meaningfully enforce the privacy rights of all Californians.

Limit Government Access to Personal Data

Privacy legislation frequently includes specific provisions that limit government access to personal data held by companies. These provisions help ensure that the government collects only the data that is necessary and appropriate for a particular criminal investigation. Without these provisions, the government would be able to collect personal data in bulk from companies, a form of mass surveillance enabled by new technologies. The Supreme Court also recently said in the *Carpenter* case that personal data held by private companies, in some circumstances, is entitled to Constitutional protection.[37] California has the strongest law about warrantless

[36] *See* Hearing on "Cybersecurity and Data Protection in the Financial Sector," H. Comm. on Financial Services 7-8 (testimony of Marc Rotenberg, Exec. Dir., EPIC) (Sept. 2011), https://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf.

[37] *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

surveillance in the nation: the California Electronic Communications Privacy Act. The AG should continue to use its authority enforce CalECPA.[38]

The proposed regulations signal that the AG intends to maintain strong data privacy protections in the CCPA for Californians. EPIC supports the AG's leadership on privacy issues and work on the proposed regulations.

Sincerely,

/s/ *Marc Rotenberg* Marc Rotenberg EPIC President	/s/ *Christine Bannan* Christine Bannan EPIC Consumer Protection Counsel
/s/ *W. Hunter Daley* W. Hunter Daley EPIC Law Clerk	

[38] Electronic Communications Privacy Act, CAL. PENAL CODE § 1546.4(b) (2016).

Message

From: David Kennedy [redacted]

Sent: 12/6/2019 8:53:35 PM

To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]

CC: 'Jerry Desmond' [redacted]; David Kennedy ([redacted]; Mark Smith [[redacted]; Joanne Ladden ([redacted]; 'David Marlow' [redacted]; 'Kevin Grodzki' [[redacted]; Stephanie Shirley [[redacted]; Nicole Vasilaros [redacted]

Subject: CCPA comments

Attachments: NMMA letter.dwd.v2.docx

David Dickerson
V.P., State Government Relations
Exec. Dir., PWIA

National Marine Manufacturers Association
650 Massachusetts Ave. NW, Suite 520 | Washington, DC 20001
[redacted] nmma.org

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

On behalf of the National Marine Manufacturers Association (NMMA), the Recreational Boaters of California (RBOC) and BoatUS, we are writing to request that you consider amending the proposed regulations implementing the California Consumer Privacy Act (CCPA) to allow for recreational marine dealers and manufacturers to exchange identifying information needed to address product warranty issues and product recalls.

NMMA is the leading trade association representing the recreational boating industry in North America. Among its many roles, NMMA is dedicated to facilitating product quality assurance. NMMA's 1,300 member companies produce more than 80 percent of the boats, engines, trailers, accessories and gear used by boaters and anglers throughout the United States and Canada.

Recreational Boaters of California (RBOC) is the nonprofit advocacy organization that promotes the interests of recreational boaters. It is important to boaters that the regulations implementing the California Consumer Privacy Act [CCPA] include provisions clarifying that essential information can be transmitted to the manufacturers of boats, engines and associated equipment so that they have the information they need to contact boat owners with important safety, repair and recall notices. As individuals whose personal information the CCPA is intended to protect, RBOC believes that boaters' information should be available to boat manufacturers for warranty and recall purposes – separate from the CCPA's provisions enabling personal information to be deleted.

BoatU.S. is the largest organization of recreational boat owners in the United States, with more than 680,000 members nationwide and more than 64,000 members in California. Boating is a healthy family activity connecting children with nature and promoting physical fitness for all. For many families, their boat is the single biggest investment they make in family recreation. BoatUS members depend upon a marine manufacturer's ability to perform accurate and complete recalls, warranty repairs and warranty eligibility. We support efforts to provide a seamless transfer of data between marine dealers and manufacturers as needed to achieve these essential services.

California ranks eighth in new boat sales, seventh in new engine sales and, with 745,640 registered boats, is the fourth largest boating state in the United States. Sales of new boats, engines and accessories totaled $718 million in 2018. Overall, recreational boating in California had an estimated direct and indirect annual economic impact of $13 billion in 2018. Clearly, hundreds of thousands of California boaters depend upon a network of manufacturers, dealers and the California state government to effectively and efficiently provide warranty information and repairs and implement product recalls if needed.

We believe the legislature intended to ensure that recreational boat owners would continue to be contacted about important safety recalls and have their boats, engines and associated equipment repaired under warranty. We request, however, that the draft regulations be clarified to give recreational marine manufacturers unambiguous certainty that the CCPA will allow them to collect the information they are required to retain under federal law for important safety, repair and recall notices.

In 2019, the Legislature passed, and the Governor signed, AB 1146 (Berman). Among the amendments this bill made to the CCPA were two standards for consumer data handling for public safety notifications related to recalls and warranties.

- 1798.105(d), relative to a consumer's request to have information deleted as it pertains to warranties and recalls.
- 1798.145(g)(1), an explicit exemption from a consumer's ability to opt-out of providing consumer identifying information to manufacturers, who thereafter use it to approve repairs under warranty or to contact owners in the event of a recall.

Chapter 1798.105(d)(1) of the CCPA states that "a business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer."

While Chapter 1798.105(d)(1) provides a broad exemption, the members of NMMA believe the information they need for warranty and recall purposes should have exactly the same protections and latitude as given to the new car industry in the CCPA. The safety of boaters and their passengers can depend upon accurate and expeditious recall actions and warranty approvals.

NMMA suggests that the explicit opt-out provisions for vehicles in 1798.145(g)(1) should be as broadly construed as possible to include recreational vessels. We encourage you to consider a regulatory interpretation that specifically allows a free flow of ownership and product information between marine dealers and manufacturers to provide the database needed for warranty verification and for recalls. This will enhance public safety by giving recreational vessel and marine engine manufacturers as complete a record as possible of product sales and ownership while applying the same provisions for the use of the information that is now in place for vehicles. For the marine industry, identifying information should include, at a minimum, the vessel's hull identification number (HIN), its make, model, model year, and the buyer's name, address and email address. Information on engines should include its serial number.

Further justification for this regulatory interpretation comes from the requirements of federal law. Manufacturers must have reliable data in order to comply with 46 U.S. Code §4310. 46 U.S. Code §4310 requires recreational boat and engine manufacturers to retain the name and contact information of the buyer of any new vessel, engine or associated product for a minimum of 10 years. Marine dealers are the only source of information about buyers and the products they purchase. Dealers provide these data seamlessly as part of the sales process.

Should a recreational vessel or engine fail to comply with the regulation or contain a defect that creates a substantial risk of personal injury to the public, 46 U.S. Code §4310 states that the manufacturer shall provide notification of the defect or failure of compliance to the original purchaser, and subsequent owners if known. This mandate is rigidly enforced.

In addition to broadly interpreting 1798.145(g)(1), the draft regulations could be amended to create a class of dealers and manufacturers of recreational marine boats and engines, automobiles, off-road vehicles and motorcycles, and other products that have similar collection, retention and reporting methods and requirements.

By grouping these business sectors into a class, the regulations could standardize the collection of this information and the conditions under which these data can be transmitted between dealers and manufacturers. Creating a single standard for these retention policies would retain the public's confidence in the recall and warranty repair system.

A possible example would be:

Product information and ownership information may be retained or shared between a new product dealer and the product's manufacturer, if the product or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a repair covered by a warranty or a recall conducted pursuant to Title 49 of the United States Code, provided that the dealer or manufacturer with which that information or ownership information is shared does not sell, share, or use that information for any other purpose.

NMMA, RBOC and BoatUS would welcome an opportunity to work with the California Office of the Attorney General to write and implement such a regulation. For questions or concerns, please contact us using the contact information, below.

David Dickerson
Vice President, State Government Relations
National Marine Manufacturers Association
650 Massachusetts Ave NW #645
Washington, DC 20001
[redacted]

Jerry Desmond
Recreational Boaters of California
925 L St #260
Sacramento, CA 95814
[redacted]

David Kennedy
BoatUS Government Affairs
5323 Port Royal Rd.
Springfield, VA 22151
[redacted]

Message

From: Chris Pedigo [redacted]
Sent: 12/6/2019 10:28:13 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Comments from DCN
Attachments: DCN Comments re CA AG CCPA Regulations Final 2019-12-06.pdf

To Whom It May Concern –

Please find the attached comments from Digital Content Next regarding the proposed regulations for the California Consumer Privacy Act. Please let me know if you have any questions about these comments or would like the comments delivered in a different format.

Sincerely,

--
Chris Pedigo
SVP, Government Affairs
Digital Content Next
[redacted]
@Pedigo_Chris

Follow us on Twitter: @DCNorg
Sign up for our weekly newsletter, InContext, for insights in digital media.

DIGITAL CONTENT NEXT

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: California Consumer Privacy Act Regulations

Dear Attorney General,

We appreciate the opportunity to comment on the regulations proposed by your office to implement the California Consumer Privacy Act (CCPA). Founded in 2001 as the Online Publishers Association, Digital Content Next (DCN) is the only trade organization in the U.S. dedicated to serving the unique and diverse needs of high-quality digital content companies which enjoy trusted, direct relationships with consumers and marketers. DCN's members are some of the most trusted and well-respected media brands that, together, have an audience of 256,277,000 unique visitors or 100 percent reach of the U.S. online population[1]. In layman's terms, every person in the U.S. who goes online will visit one of our member companies' websites at least one time each month.

Do Not Sell

As we noted in our letter[2] dated November 7, when a consumer activates their Do Not Sell right, the CCPA and your proposed regulations would require 3rd party companies on a website or app to limit their data collection and use to the role of a service provider, which means they could not use data about the consumer except on behalf of the website or app publisher as defined by contract with the publisher. For example, Facebook and Google would need to stop collecting data about consumers via the "like" button and ad serving technologies, respectively. Unless and only when the consumer intentionally interacts with those services, Google and Facebook should be considered third parties. Given our experience with

[1] *comScore Media Metrix Multiplatform Custom Audience Duplication*, December 2017 U.S.

[2] https://digitalcontentnext.org/wp-content/uploads/2019/11/DCN-letter-to-CA-AG-2019-11-07.pdf

implementation of the General Data Protection Regulation (GDPR) in Europe, it is important that this point be clear. We are concerned that some third parties may try to implement creative interpretations of the CCPA which would run counter to the law and consumer expectations.

Disclosure Requirements

We are concerned that the requirements for disclosure to consumers of data collection practices, taken as a whole, may be overwhelming for consumers trying to understand how their data is being used and counterproductive to the goals of the CCPA. Specifically, Section 999.308 (b)(1)e.1 of the proposed regulations would require companies to "state whether or not the business has disclosed or sold any personal information to third parties for a business or commercial purpose in the preceding 12 months." According to Section 1798.140 (d) of the CCPA, business purposes include "auditing," "detecting security incidents," "debugging," "short-term, transient use," "customer service" and "internal research" among other things. The California Legislature wisely carved out these activities from the scope of a "sale" because they are examples of benign data collection and use that are necessary to providing a service to consumers. We are concerned that, by lumping "business purposes" with "commercial purposes" in the disclosure requirement, the benign activities under "business purposes" may be unfairly characterized. Consumers may be confused about whether "business purposes" would be within the scope of the CCPA's Do Not Sell right.

In addition, we are concerned about the disclosure requirements in Section 999.317 (g), which require a "business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall" disclose several metrics related to the number of consumer requests to know, delete and opt out along with the median number of days it took the business to substantively respond. We believe the threshold of "4,000,000 or more consumers" is very low particularly for businesses that primarily interact with consumers online. According to ComScore, the top 5 most visited "businesses" online each attracted over 200 million consumers in September 2019[3] alone. While we support the goal of providing transparency for consumers especially with regard to how big data companies are complying with the CCPA, we are concerned that this obligation will unintentionally fall on small businesses with limited resources. We encourage you to significantly raise the threshold at least for businesses that primarily interact with consumers online or focus on businesses which collect data on consumers across a broad range of unaffiliated websites.

Flexibility for Service Providers

Service providers should use data consistent with their contracts with publishers, thus we applaud the proposed regulations' allowance in Section 999.314 (c) for service providers to "combine personal information received from one or more entities to which it is a service provider…to detect security incidents, or protect against fraudulent or illegal activity." Fraudulent or criminal actors often pose as real consumers to either engage in fraudulent

[3] https://www.comscore.com/Insights/Rankings

advertising or exploit security weaknesses. Allowing publishers to use service providers to weed out these bad actors protects consumers and helps build trust in the internet marketplace.

90-Day Notification Requirement

Section 999.315 (f) requires businesses 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 consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information." For example, in a typical behaviorally-targeted advertisement on a website, there are multiple companies involved in serving the ad. In order to comply with Section 999.315 (f), all of the companies involved in serving the ad, assuming it qualified as a "sale," would need to keep a record of which consumer saw which ad along with the specific pieces of data that were collected. We are concerned that this requirement would be difficult to implement and would inadvertently require businesses to collect additional data about consumers. We urge you to strike this 90-day notification requirement.

Industry Solutions

Over the coming weeks and months, there will be significant discussion about developing an industry-wide solution for compliance with the CCPA. Recently, the Interactive Advertising Bureau (IAB) issued such a proposal[4] for consideration. While we are still carefully examining the details of the proposal and awaiting additional documentation, we want to publicly support the basic approach of the IAB framework as it relates to the implementation of the consumer's Do Not Sell (DNS) right. When a consumer exercises their DNS right, the IAB framework requires that the business (e.g. publisher) pass along a signal to all downstream companies that indicates the consumer has opted out of the sale of their information. When those downstream companies receive the signal, they would immediately conform their data collection and use practices to the role of a "service provider," meaning those downstream companies could not use data for any secondary purpose including the building of a profile about that consumer. We believe this approach satisfies the letter and spirit of the CCPA to give consumers control of how their data is collected and used. This approach also allows for small and large businesses to operate with the same understanding of the law's requirements and would prevent dominant companies from abusing their market position to circumvent the CCPA.

Browser and Device-Level Signals

Section 999.315 (c) notes 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" should be considered a valid signal. DCN appreciates the desire to find simple solutions for consumers who want to indicate their privacy preferences particularly given the likelihood of multiple consumer options, as well as the involvement of both consumer-facing companies and those that provide functionality from behind the scenes including those that track consumers outside of a consumer's reasonable expectation. These

[4] https://www.iab.com/guidelines/ccpa-framework/

signals can be useful for consumers as they are persistent and easy to use. They can also be useful for consumer-facing companies as the signals are sent in real-time to all downstream companies. However, there is no widely-adopted industry standard for the messaging and design of these signals that ensures the signals accurately reflect the expressed preferences of consumers. In the absence of additional guidance, we are concerned that there will be a patchwork of signals which could be confusing or misleading for consumers. In addition, we are concerned that some dominant platform companies may develop their own signals in an effort to unfairly tilt the competitive landscape in their favor. Given the potential for confusion and abuse, we encourage your office to rely on the work of-independent, multi-stakeholder, standard-setting groups[5] to develop guidelines and/or an approval process for how privacy controls such as browser and device-level signals can operate and how they can be advertised to consumers. By developing some common rules for the road, your office will be better able to identify anti-competitive behavior, industry will have more confidence in the signals and consumers will have a better understanding of the benefits and limitations.

Conclusion

Thank you for the opportunity to comment on the proposed regulations regarding the CCPA. We applaud your thoughtful approach to the practical questions for implementing this important law. Please do not hesitate to reach out directly to us with any questions or comments.

Sincerely,

Jason Kint
CEO
Digital Content Next

Chris Pedigo
SVP, Government Affairs
Digital Content Next

[5] World Wide Web Consortium (W3C) https://www.w3.org/2011/tracking-protection/

Message

From: Matt Gardner [redacted]
Sent: 12/7/2019 12:18:58 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Comments
Attachments: CCPA Comments CA Tech Council 12.6.19.pdf

To The Privacy Regulations Coordinator:

Comments from the California Technology Council in the attached PDF.

Thank you,
Matt Gardner, CEO
California Technology Council

CALIFORNIA
TECHNOLOGY COUNCIL

6 December 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

To Whom It May Concern:

On behalf of the California Technology Council and, in particular, our California Cybersecurity Information Sharing Organization and the members we have most concerned with privacy and cybersecurity, we appreciate the opportunity to provide comments to the draft California Consumer Privacy Act (CCPA) regulations issued by your office in October of this year.

As written, the law and draft regulations create confusion for business and consumers, add layers of unnecessary and intended regulation in business-to-business (B2B) commerce, impose costs that are too high, and layer additional requirements beyond what is already in the CCPA, all of which heighten the difficulty for small and medium size business to develop in good faith a compliance regiment in a very narrow window of time given the complexity of the CCPA. It is our understanding that the finalized regulations will not be released before the spring of 2020, with an enforcement date of July 1, 2020. That only provides for a few months for small and medium size businesses once the final regulations are made public.

We appreciate your work to reconcile the CCPA and the many "clean-up" bills that were passed to clarify the original bill, but California business owners are similarly struggling to understand their compliance requirements. With less than a month to go, business owners are largely unsure of where to allocate resources, what kind of consultants are needed in order to ensure compliance, and what software is needed to upgrade their systems.

Speeding towards January 1, businesses are being required to fundamentally change their operations to become compliant with a law very few can understand, at very high cost. As determined by the economic impact assessment prepared for your office, implementation of CCPA, as passed by the Legislature, will cost California businesses $55 billion, equivalent to 1.8% of the state's Gross Domestic Product, in just initial compliance costs. And the estimated cost of $50,000 for small business to hire a lawyer, engage a technology business, buy software, and maintain records and respond to requests is more than many small and medium size businesses can afford.

We are concerned that the regulations exceed the requirements in the CCPA. Rather than facilitating and encouraging compliance, we believe the current regulations will lead to more confusion and noncompliance. The regulations appear to require business to comply with heightened notice requirements, establish enhanced privacy policies, and produce more information to consumers upon request for personal information. Additionally, the regulations impose new requirements for responding to consumer requests without considering the time necessary to verify the request. This is exemplified by the new requirement to calculate the value of consumer data. Forcing businesses to calculate the value of consumer data is beyond what is written in statute. Further there are too many variables that go into this calculation making any value created subjective and unreliable.

The regulations also fail to provide enough direction around establishment of an opt-out policy. Small businesses subject to the CCPA need more clarification of the opt-out and opt-in requirements in order to present consumers with a legally sufficient and effective means of establishing their privacy preference.

We are concerned about the broad definition of personal information and the requirement that a business identify all personal information reasonably capable of being linked to a consumer. Many businesses voiced concern about the possibility that consumer requests will create privacy issues by requiring a business to connect disparate pieces of information to respond to the consumer request.

This policy seems inconsistent with the purpose of protecting privacy, potentially actionable from a security standpoint and incredibly time-consuming for a business trying to meet consumer needs. Also, the regulations are still confusing regarding household information. We are mandated to protect individual privacy but required to release household information without a means of verifying the identity of the requestor.

The regulations further introduce a process for businesses to give notices in person and gives individuals the ability to submit requests in person. This additional requirement is concerning for small business owners who might have not the bandwidth or expertise to comply with this process. The issues here are expounded by the requirement that business compile and post annual metrics from the previous year. Not only is this an onerous requirement but risks unfairly portraying small businesses in an unfavorable light despite good faith efforts to comply. This would especially be the case for small businesses who are being forced into fundamental changes of their business while under an expedited timeline.

We are also concerned that the new private right of action will lead to a cottage industry of phony complaints, much like the scams associated with the Americans with Disabilities Act (ADA). The misuse of the ADA took nearly a decade to reform and drove many small business owners into financial trouble.

Here, the statutory damages that will arise from even a small data breach will be staggering -- forcing many businesses to settle rather than fighting a costly legal battle over the reasonableness of their data security procedures. Worse, recovery of damages does not require a plaintiff to prove that they were actually been damaged by the breach.

We are concerned that the regulations and the passage of AB 25 provide a temporary solution for handling information relating to employees. While some of the CCPA requirements were deferred, other provisions of the CCPA will take effect in January. The regulations attempt to clarify the requirements imposed on a business but have left many unsure about whether to continue to keep employees' files for the purpose of determining compensation, reviewing performance, handling possible violations of business policy or keeping records of leave and other operational matters. Much of the employee information in question is contained in company software. Given the uncertainty around a one year "fix" and the need to comply with remaining requirements, business will need to decide how to modify their current procedures or simply replace their current system. This uncertainty makes compliance more complicated and costly.

For many small businesses, digital advertising has become the great equalizer in competing with larger entities that have a national footprint or a big traditional advertising budget. Our members are unclear about whether digital advertising will still be an effective means of reaching customers.

Small businesses have limited resources. We are not interested in accumulating personal information, we are simply trying to connect with our customers or potential customers. The proposed rules will likely make customer acquisition more expensive for small businesses by significantly limiting the availability and effectiveness of targeted advertising. Clarity around permissible interactive engagement would help us to understand how we can operate within the limitations of the law.

We strongly support efforts to protect consumer privacy. But in doing so, we also must ensure that the rules governing these protections are laid out in a way that allows businesses to reasonably and successfully comply with the law. Meanwhile, it is worth noting that state agencies such as the Department of Motor Vehicles have been exempted from these requirements to protect consumer information and end certain practices of selling consumer data. The on-going efforts of the California DMV to monetize the information of California consumers - information collected using the full force of state requirement and gathered on forms with which citizens must comply - has generated tens of millions in revenue to DMV through sale to private businesses.

Protecting consumers privacy is an important and laudable goal – but not a goal to be pursued at any cost. Rather, we believe the goal should be to pursue sensible, cost-effective privacy rules. Consumers count on us to protect their privacy; however, they also rely on us to maintain a functioning economy as well as ensure their access to internet services. We trust that as your office finalizes the regulations, you will ensure that all these goals can be achieved.

Sincerely,

Sincerely,

Matt Gardner

Matt Gardner
Chief Executive Officer

Message

From: Julian Peterson [redacted]
Sent: 12/6/2019 10:00:57 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Draft Regulations Comments
Attachments: CCPA Comments.pdf

To Whom It May Concern,

Please see the attached correspondence.

Best,

Julian Peterson
Corporate Counsel

1400 Valley House Drive, Suite 120
Rohnert Park, CA 94928

CONFIDENTIAL:
The information contained in this email communication is confidential and may be privileged pursuant to attorney-client privilege and/or work-product doctrine. Unauthorized use, disclosure or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by return email, or call 707.664.5873 and destroy all copies of this communication, including attachments

TRADITIONAL MEDICINALS

6 December 2019

Submitted via PrivacyRegulations@doj.ca.gov

Re: Draft California Consumer Privacy Act Regulations

To Whom It May Concern:

I submit these comments as a supporter of the values embodied by the California Consumer Privacy Act (CCPA) and commend the state of California for taking these important steps. Regarding specific issues of concern:

1. I request that you remove the ability of "authorized agents" to make requests on behalf of consumers. Allowing such authorized agents, even with the mechanisms proposed in the draft regulations, opens a huge potential for fraud and misuse of consumer information and complicates the consumer-verification process – frustrating the very purpose of the CCPA.
2. I request that you provide a clear timeline for a consumer to provide verification for their request. While the draft regulations allow for denial of a request and also allow a total of 90 days for a business to respond to a request, it is not clear whether a company must wait the full 90 days, including writing the unverified consumer explaining that there an extension is needed, before denying the request. Without such a timeline/process, a company is left in unknown territory and forced to devote resources to a potentially fraudulent consumer request.
3. I request clarification as to the data management aspect of complying with a consumer's request to know or request to delete. Specifically, the amount a time a company must retain records on the company's compliance with a consumer's request to know and/or delete.
4. While this is beyond the scope of the draft regulations, I would request that the exception for employee information be made permanent. Employee information is not used by companies as a commodity but rather as a necessity for insurance; payroll and accounting purposes; Equal Employment Opportunity Commission compliance; and a host of other legally-mandated reasons. As a result, in virtually all cases the company will be unable to delete the information if requested by a consumer pursuant to the CCPA process, causing unmet expectations for the consumer and wasted time and resources for the company.

Best regards,

Julian Peterson

Julian Peterson
Corporate Counsel

Message

From:	Kingman, Andrew [redacted]
Sent:	12/6/2019 8:24:15 PM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject:	CCPA Proposed Regulations - Comments on Behalf of Pindrop Security, Inc.
Attachments:	Pindrop AG Comments - Proposed Regs with Appendix A (signed 12-06-19).pdf

Good afternoon,
Attached, please find targeted comments on provisions relating to Service Providers, Requests to Know, and Verification of Requests submitted by Pindrop Security, Inc.

Please do not hesitate to contact me if you have any questions.

Respectfully,
Andrew A. Kingman

Andrew Kingman
Senior Managing Attorney

[redacted]

DLA PIPER

DLA Piper LLP (US)
33 Arch Street, 26th Floor
Boston, Massachusetts 02110-1447
United States
www.dlapiper.com

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.

pindrop

COMMENTS TO ATTORNEY GENERAL

December 5, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 Spring St.
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: Comments on Title 11(1)(20): CCPA Proposed Text of Regulations

Dear Attorney General Becerra and Staff,

With January 1, 2020 rapidly approaching, Pindrop Security, Inc. continues to put in place the necessary compliance tools to ensure that the California Consumer Privacy Act (CCPA) is integrated as smoothly as possible into our existing operations. As a leading provider of anti-fraud products and services in call centers for financial institutions, insurance, retail, and government organizations, we are on the cutting edge of detecting and preventing identity theft and other types of fraudulent activity, and thereby protecting the privacy of California residents.

We know these things to be true: 1) Fraudsters are consistently innovating new methods to compromise individuals' identities and personal information; 2) Biometrics – specifically, voice authentication – offers the best protection for call centers against these new methods (which include audio manipulation and sophisticated routing of phone data to mask the true location and identity of the caller); and 3) New privacy laws, laudable for their commitment to increased consumer control and transparency, concurrently offer significant opportunities for these bad actors as companies, trying in good faith to comply with these complex statutory requirements, release large amounts of consumer data upon request.

Pindrop offers comments on three sections of the Proposed Regulations (draft rules):

- First, we address the Section 999.314 requirements that pertain to Service Providers and propose modifications that help reduce the risk of identity theft.
- In Section 999.313, we also propose the addition of stronger anti-fraud exemption language for Requests to Know, so that consumers are protected from identity theft and businesses are protected from class action lawsuits for data breaches.

- Finally, we incorporate our comments from June 2019 and seek to institute "MFA 2.0" as a per se reasonable and secure method for verifying consumers who are requesting sensitive information pursuant to Section 999.323 and .325.

I. <u>Section 999.314 – Service Provider Requirements</u>

Pindrop recognizes the commitment that your office has shown in the draft rules to strengthening the dangerously weak anti-fraud protections in the existing CCPA statute. To that end, we emphatically support retaining the provision in .314(c) that allows service providers to pool consumer data for identity theft and anti-fraud purposes. Nearly every large business outsources some degree of its security to service providers who specialize in detecting and preventing cybercrime. Allowing these service providers to keep pace with cybercriminals by sharing this information across clients and industries is critical to the health of these ecosystems. Conversely, forcing service providers to silo this info ties both hands behind their backs, and puts both consumers and companies at significant and needless risk.

Additionally, we propose, with regard to identity theft and anti-fraud detection services, the deletion of .314(d), which indicates that service providers must respond to some degree to a consumer request. We believe this is counterproductive to the concept of a service provider – an entity acting at the direction of a business – because it does not permit the business to decide how to respond. Moreover, many companies have been readying for CCPA to take effect by, in part, modifying contracts with vendors. Often these contracts specify that service providers are only to assist the business in responding to a request; the draft rules should not complicate this arrangement. This is an untenable position and we would request paragraph (d) be deleted.

We request clarifying language to create synchronization between paragraphs (c) and (d) in the anti-fraud and data security sectors. Specifically, we would propose that paragraph (d) be amended to add language after the last sentence stating:

> **A service provider that combines personal information received from one or more entities to which it is a service provider to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity, shall not be required to respond to a consumer who submits a request to know or request to delete from a consumer.**

This language is necessary for operational purposes. If a service provider such as Pindrop combines personal information received from multiple entities, it is nearly impossible to comply with the current language requiring that the service provider "when feasible, provide the consumer with contact information" for the business from which it receives the personal information.

It is also necessary for security purposes. Under the draft rules as written, we believe that fraudsters will attempt to create "maps" of security-focused service providers by submitting Request to Know and seeing where these service providers direct them. It will allow fraudsters to get an idea of who has their information and, by negative inference, who is still vulnerable. Less sophisticated fraudsters may well randomly target access requests to companies, seeing who will respond and how. Adding the exemption above is a narrowly-tailored solution to this current loophole.

II. Section 999.314 – Requests to Know (Data Security Exemption)

Again, we appreciate your office's concern for data security and consumer fraud that is evident in this section. However, we believe this section could be made stronger. Currently, .314(c)(3) provides an exception to a Request to Know when such disclosure "creates a substantial, articulable, and unreasonable risk" in three scenarios: (1) to the security of that personal information; (2) to the consumer's account with the business; or (3) to the security of the business's systems or networks.

Unfortunately, a business is required to respond under the draft rules even if there is a risk to the consumer's safety, since that would not fall under one of the three scenarios stated above. Moreover, from an anti-fraud perspective, there is little difference in risk to a consumer or business from a Request to Delete (for which the CCPA includes a fraud exemption) and a Request to Know. For these reasons, we recommend deleting (c)(3) and replacing it with the following language similar to the deletion exemption found in 1798.105(d)(2), but with a sharper focus on protecting consumers: "A business shall not respond to Request to Know to the extent that the disclosure of such personal information inhibits a business's ability to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, prosecute those responsible for that activity, or safeguard consumers or consumer personal information."

Pindrop is concerned that the maintenance of the current set of circumstances in which a business can refuse to respond to a Request to Know only in certain circumstances when there is "unreasonable" risk shifts the burden of decision-making from the front lines of cyber professionals to compliance attorneys who may not be in the best position to determine what a) is reasonable, and b) constitutes a risk to the security of the network systems.

Instead, we recommend a standard that provides strong protections for both the consumer and the business, and allows businesses to listen to their security service providers and security professionals about who is asking for the information and whether that request is legitimate.

III. Verification of Requests

Attached as Appendix A are Pindrop's initial comments to the regulatory process, submitted in June 2019. In that document, we described our advances in multifactor authentication as "MFA 2.0," stating:

> **MFA 2.0 is a system of multifactor authentication that combines at least two of: 1) something you are; 2) something you have; and 3) something you do. This third factor – something you do – replaces the factor "something you know," which has been the dominant factor in MFA since MFA's inception.**
>
> **The ability to incorporate something you do into an MFA process represents a dramatic, generational improvement in the ability of companies to safeguard customer and employee data, and also offers possibilities to more securely authenticate a consumer in the context of his or her individual transactions.**

We propose amending the draft rules to incentivize businesses to adopt MFA 2.0 in certain situations – when verifying a request for sensitive information; as a per se "reasonable security measure" to "detect fraudulent activity; and as a sufficient method of verifying non-account holders matching two points of data to a reasonable degree of certainty.

a. Amend .323(b)(2) to add a biometric information exemption

The draft regulations state that a business shall "[a]void collecting the types of personal information identified in Civil Code section 1798.81.5(d), unless necessary for the purpose of verifying the consumer." In October, AB 1130 was signed by the Governor, adding "biometric information" as a data element to the state breach notification statute.

This update to the breach notification statute does not make sense as a basis to exclude biometric data as an option for verifying consumers. To the contrary, biometrics stand as one of the most, if not the most, secure methods of authentication that currently exist. Furthermore, these data are less risky than the other data elements in .1798.81.5. Unlike social security numbers, for example, they cannot be used on their own to imitate someone's identity or deduce someone's health or insurance status. At the same time, inclusion of biometric data in AB 1130 risks disincentivizing collection of biometric data through the language in .323(b)(2). For this reason, as a first step, we propose adding the following sentence to 323(b)(2): "This requirement shall not apply to biometric information."

b. Amend .323(d) to add MFA 2.0 as a sufficient "reasonable security measure."

The draft rules additionally require the implementation of "reasonable security measures to detect fraudulent identity-verification activity." Pindrop offers the following sentence as an amendment: "The use of multifactor authentication using at least of two of the following: 1) something you are; 2) something you have; and 3) something you do, shall be considered a reasonable security measure."

Currently, there is little guidance on what constitutes a "reasonable security measure." The most recent guidance was that issued in 2016 by then-Attorney General Kamala Harris (which endorsed MFA 1.0). However, even in three short years, hackers and fraudsters have gained an exponentially higher level of sophistication. Businesses should be able to know with certainty that they are using a safeguard that allows them to comply with the draft rules.

c. Use MFA 2.0 as verification for non-account holders.

Finally, the draft rules set out what constitutes a reasonable authentication for Requests to Know specific pieces of information, but this authentication is very burdensome for accurate identifiers. They state in .325(c) that in order to verify a request for specific pieces of information, it verify the request to a "reasonably high degree of certainty...[which] may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business," in addition to a declaration under penalty of perjury signed by the consumer requesting the information.

Pindrop proposes that in addition to this option, businesses be given the option to verify a consumer using MFA 2.0. This seamless, frictionless experience over the phone allows a business to instantly know whether a consumer is a fraudster or legitimate. This is because MFA 2.0 engages unique, one-time authentication sequencing, meaning that efforts to forge, replicate, or guess at an authentication factor stand an exponentially lower chance of success. The ability to pair an identifier such as a highly developed voiceprint, and also the device proximity that MFA 2.0 has the potential to include, means that any individual transaction, as well as overall account security, becomes secure to a degree that the current cybersecurity ecosystem has yet to fully appreciate.

In conclusion, Pindrop believes that by using narrowly tailored language in targeted sections of the draft rules, your office has an opportunity to meaningfully increase the cybersecurity and consumer protections that are included in the CCPA without creating loopholes that concern privacy advocates.

Pindrop thanks you for your time and consideration. We would be delighted to discuss these issues further.

Clarissa Cerda
General Counsel
Pindrop Security, Inc.

APPENDIX A

pindrop

COMMENTS TO ATTORNEY GENERAL

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 Spring St.
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: 1798.185(a)(7) – Multifactor Authentication 2.0

Introduction

As California ushers in a new era of consumer privacy with the California Consumer Privacy Act's (CCPA) passage, the Attorney General and other policymakers should take advantage of this moment by reassessing what constitutes effective security for authenticating requests for access to consumer information. With increased transparency in how companies handle consumer information comes a concurrent responsibility for businesses, government, and non-profits to incorporate protections from the persistent efforts of fraudsters, hackers, and other scammers who every minute are trying to acquire and exploit consumer data for their nefarious purposes.

Advances in Multifactor Authentication (MFA) can greatly increase both consumers' privacy and security. For this reason, we propose that the Attorney General's office recommend large-scale entities subject to CCPA – businesses subject to the law with more than $100 million in revenue-- adopt what we term "MFA 2.0" for requests under the CCPA to access, delete or obtain in portable format personal information.

Specifically, as the Attorney General's office considers rules related to verifiable consumer requests under § 1798.185(a)(7), it should recommend the use of MFA 2.0 as technology that can help appropriately and quickly authenticate a consumer. This is especially important here because the CCPA requires turning over all "specific pieces" of personal information upon receipt of a verifiable request. This creates a significant avenue for fraudsters to obtain consumer data, including sensitive information such as government ID and financial account numbers. In this context, it is *critical* that strong authentication processes are in place. And, in order to secure personal data more generally, businesses should have effective tools in their toolbox to frustrate fraudsters' efforts.

On the consumer side, technology is progressing quickly, and MFA 2.0 offers unparalleled opportunities to provide a far greater degree of consumer authentication and data security than currently exists.

Finally, we discuss how MFA 2.0 is uniquely equipped to counteract the nascent but pervasive effect of "deepfakes."

What is MFA 2.0?

MFA 2.0 is a system of multifactor authentication that combines at least two of: 1) something you are; 2) something you have; and 3) something you do. This third factor – something you do – replaces the factor "something you know," which has been the dominant factor in MFA since MFA's inception.

The ability to incorporate something you do into an MFA process represents a dramatic, generational improvement in the ability of companies to safeguard customer and employee data, and also offers possibilities to more securely authenticate a consumer in the context of his or her individual transactions.

How Can MFA 2.0 Help Enterprise Businesses Comply with CCPA and Enhance Its Cybersecurity?

As stated above, we propose that the Attorney General recommend the adoption of MFA 2.0 for enterprise-level businesses with in-state revenues over $100M, and who use a phone line to receive verifiable consumer requests. These businesses should utilize a minimum of two, but preferably three of the authentication factors. Doing so provides a highly certain, and consequently strong, degree of authentication to the transaction.

As an example, Phoneprinting is an enterprise technology that analyzes the entire audio signal of a call, including the one-time characteristics of the call's path. It combines this information with extractions of non-voice audio features such as the signal-to-noise ratio and dropped frames to help determine the device type, location, and carrier. As Gartner states in its 2018 Report "Don't Let the Call Center Be Your Fraud Achilles Heel,"[1] "Phoneprinting...can identify anomalies and the unusual repetition of background noise across multiple calls" and is "often effective at detecting fraud." By establishing a unique signature that combines authentication factors from both the caller (voiceprint) and the device (phoneprint), institutions are able to

[1] Gartner, Inc. *Don't Let the Contact Center Be Your Fraud Achilles Heel*, Published December 18, 2018, available at https://www.gartner.com/doc/3895904/dont-let-contact-center-fraud

make real-time risk assessments to determine whether a caller is a fraudster, or a legitimate customer, even for first-time callers whose voice may not be in a database. This type of authentication improves efficiency, accuracy, and most importantly, the security of consumer information. Institutions can have a much higher degree of confidence that the caller is verified, rather than a fraudster who has obtained legitimate KBA information (such as a former street address or vehicle) to obtain, e.g., a consumer's checking account and routing numbers.

How Can MFA 2.0 Enhance Consumer Security and Privacy?

As hackers have become more sophisticated, knowledge-based authentication (KBA) no longer provides an adequate level of protection for consumers and institutions as a frontline MFA factor. That is because KBA focuses on static data elements, such as birth date, a former address, or a mother's maiden name. These data elements are frequently available via public information on social media platforms, real estate websites, and from services that compile public records for a fee, and often only one or two correct answers to these questions are needed to access an account.[2] As individuals' data increasingly becomes available on the dark web, these elements are even more readily accessible. The 2015 IRS breach was a result of precisely this point of failure in the system – hackers were able to correctly guess the knowledge-based elements, and as a result, the IRS suffered a breach of 100,000 taxpayer accounts.

Even as consumer information is appearing for sale and use on the black market – some estimates put the number of consumer records available on the black market at 1.4 *billion*[3] - consumers are valuing their own data more and more. A 2016 study by the Ponemon Institute indicated that 75% of respondents stored either a moderate or significant amount of personal data on their mobile phones.[4] Moreover, respondents valued the data on their phones at an average of $14,000, and respondents who took steps to secure the data on their phone valued their data at $16,268.

Surely, the amount of data consumers bring with them every day, and the value they place on that data, has only increased since 2016. And while fraudsters are becoming more sophisticated, the very devices that they seek to penetrate are the devices that have the potential to offer the greatest degree of security when they incorporate MFA 2.0.

[2] https://www.itprotoday.com/identity-management-access-control/security-sense-how-do-you-do-knowledge-based-authentication-when
[3] https://www.pymnts.com/news/security-and-risk/2018/retire-knowledge-based-authentication/
[4]https://www.ponemon.org/local/upload/file/How%20much%20is%20the%20data%20on%20your%20mobile%20device%20worth%20Final%2010.pdf

MFA 2.0's authentication goes far beyond the sophistication with which current hackers and fraudsters operate. By engaging unique, one-time authentication sequencing, efforts to forge, replicate, or guess at an authentication factor stands an exponentially lower chance of success. The ability to pair an identifier such as a highly developed voiceprint, and also the device proximity that MFA 2.0 has the potential to include, means that any individual transaction, as well as overall account security, becomes secure to a degree that the current cybersecurity ecosystem has yet to fully appreciate.

MFA 2.0 Can Support Future Public Policy Challenges

In the coming months and years, "deepfakes" – the use of synthetic audio files derived from actual voice recordings, synced with real (sometimes modified) video, will become a pressing public policy and social issue.[5] While they are currently somewhat rudimentary, increasing sophistication with video and audio development have the potential to wreak havoc with the concept of a democracy based on facts. As this progression occurs, MFA 2.0 will be the single most effective tool to combat these efforts, as it will be able to quickly and accurately determine the authenticity, or lack thereof, of an individual's voice and device origin. Recommended adoption now will help suppress and deter deepfakes in the future.

Next Steps – CCPA and Beyond

The California Attorney General's Office is no stranger to providing guidance on how businesses can best protect themselves and their customers from data breaches. In 2016, this office, under the leadership of then-Attorney General Kamala Harris, issued a data breach report specifically recommending that businesses adopt MFA in order to provide sufficient data security. The report states:

> Th[e] authentication system is failing. We don't use unique passwords for each of our accounts because it would simply be too hard to remember them all...Making matters worse, many individuals do not use strong passwords that are difficult to guess.
>
> A stronger form of online authentication uses multiple factors...this form of authentication should be used by all organizations to help protect access to critical systems and sensitive data. Multi-factor authentication should also be more widely available for consumer-facing online accounts that contain sensitive personal information.[6]

[5] https://www.biometricupdate.com/201902/threat-of-deepfakes-draws-legislator-and-biometrics-industry-attention

[6] https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

The obsolescence of KBA today echoes the report's warnings about weak, commonly-used passwords just three years ago. Instead of weak passwords, KBA's decreasing relevance and inherent weakness derives from easy-to-guess questions and readily attainable information that informs common questions. Attempting to improve KBA by creating more unique or harder questions means these questions will also be harder to remember, and inevitably create greater friction for a customer trying to log on to an app, or interact with a customer-service business function. Even "easy" KBA questions can be difficult to remember – a 2015 study by Google revealed that only 47% of respondents could remember what they put down as their favorite food a year earlier, but that hackers could guess that food (pizza) nearly 20% of the time.[7]

Your office has been charged, in part, to issue rules regarding consumer verification so that businesses can properly identify consumers as they exercise their rights. This presents grave issues of security and authentication. We request that the Attorney General's office issue guidance recommending the use of MFA 2.0, both in this rulemaking and in other forthcoming publications that examine issues of data privacy and security.

It is not a question of whether MFA 2.0 is effective – it is a question of how quickly it will be adopted. California can help chart a course toward the adoption of virtually instant, virtually impenetrable consumer authentication, and we urge the Attorney General to seize this opportunity.

For these reasons, we respectfully request that your verifiable request rules under § 1798.185(a)(7) recommend use of MFA 2.0 as a method to verify requests, and that subsequent cybersecurity guidance do so as well.

Clarissa Cerda

Clarissa Cerda
General Counsel
Pindrop Security, Inc.

[7] https://www.forbes.com/sites/forbestechcouncil/2018/01/22/everybody-knows-how-knowledge-based-authentication-died/#64b13cee4eee

APPENDIX A

pindrop

COMMENTS TO ATTORNEY GENERAL

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 Spring St.
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: 1798.185(a)(7) – Multifactor Authentication 2.0

Introduction

As California ushers in a new era of consumer privacy with the California Consumer Privacy Act's (CCPA) passage, the Attorney General and other policymakers should take advantage of this moment by reassessing what constitutes effective security for authenticating requests for access to consumer information. With increased transparency in how companies handle consumer information comes a concurrent responsibility for businesses, government, and non-profits to incorporate protections from the persistent efforts of fraudsters, hackers, and other scammers who every minute are trying to acquire and exploit consumer data for their nefarious purposes.

Advances in Multifactor Authentication (MFA) can greatly increase both consumers' privacy and security. For this reason, we propose that the Attorney General's office recommend large-scale entities subject to CCPA – businesses subject to the law with more than $100 million in revenue-- adopt what we term "MFA 2.0" for requests under the CCPA to access, delete or obtain in portable format personal information.

Specifically, as the Attorney General's office considers rules related to verifiable consumer requests under § 1798.185(a)(7), it should recommend the use of MFA 2.0 as technology that can help appropriately and quickly authenticate a consumer. This is especially important here because the CCPA requires turning over all "specific pieces" of personal information upon receipt of a verifiable request. This creates a significant avenue for fraudsters to obtain consumer data, including sensitive information such as government ID and financial account numbers. In this context, it is *critical* that strong authentication processes are in place. And, in order to secure personal data more generally, businesses should have effective tools in their toolbox to frustrate fraudsters' efforts.

On the consumer side, technology is progressing quickly, and MFA 2.0 offers unparalleled opportunities to provide a far greater degree of consumer authentication and data security than currently exists.

Finally, we discuss how MFA 2.0 is uniquely equipped to counteract the nascent but pervasive effect of "deepfakes."

What is MFA 2.0?

MFA 2.0 is a system of multifactor authentication that combines at least two of: 1) something you are; 2) something you have; and 3) something you do. This third factor – something you do – replaces the factor "something you know," which has been the dominant factor in MFA since MFA's inception.

The ability to incorporate something you do into an MFA process represents a dramatic, generational improvement in the ability of companies to safeguard customer and employee data, and also offers possibilities to more securely authenticate a consumer in the context of his or her individual transactions.

How Can MFA 2.0 Help Enterprise Businesses Comply with CCPA and Enhance Its Cybersecurity?

As stated above, we propose that the Attorney General recommend the adoption of MFA 2.0 for enterprise-level businesses with in-state revenues over $100M, and who use a phone line to receive verifiable consumer requests. These businesses should utilize a minimum of two, but preferably three of the authentication factors. Doing so provides a highly certain, and consequently strong, degree of authentication to the transaction.

As an example, Phoneprinting is an enterprise technology that analyzes the entire audio signal of a call, including the one-time characteristics of the call's path. It combines this information with extractions of non-voice audio features such as the signal-to-noise ratio and dropped frames to help determine the device type, location, and carrier. As Gartner states in its 2018 Report "Don't Let the Call Center Be Your Fraud Achilles Heel,"[1] "Phoneprinting…can identify anomalies and the unusual repetition of background noise across multiple calls" and is "often effective at detecting fraud." By establishing a unique signature that combines authentication factors from both the caller (voiceprint) and the device (phoneprint), institutions are able to

[1] Gartner, Inc. *Don't Let the Contact Center Be Your Fraud Achilles Heel*, Published December 18, 2018, available at https://www.gartner.com/doc/3895904/dont-let-contact-center-fraud

make real-time risk assessments to determine whether a caller is a fraudster, or a legitimate customer, even for first-time callers whose voice may not be in a database. This type of authentication improves efficiency, accuracy, and most importantly, the security of consumer information. Institutions can have a much higher degree of confidence that the caller is verified, rather than a fraudster who has obtained legitimate KBA information (such as a former street address or vehicle) to obtain, e.g., a consumer's checking account and routing numbers.

How Can MFA 2.0 Enhance Consumer Security and Privacy?

As hackers have become more sophisticated, knowledge-based authentication (KBA) no longer provides an adequate level of protection for consumers and institutions as a frontline MFA factor. That is because KBA focuses on static data elements, such as birth date, a former address, or a mother's maiden name. These data elements are frequently available via public information on social media platforms, real estate websites, and from services that compile public records for a fee, and often only one or two correct answers to these questions are needed to access an account.[2] As individuals' data increasingly becomes available on the dark web, these elements are even more readily accessible. The 2015 IRS breach was a result of precisely this point of failure in the system – hackers were able to correctly guess the knowledge-based elements, and as a result, the IRS suffered a breach of 100,000 taxpayer accounts.

Even as consumer information is appearing for sale and use on the black market – some estimates put the number of consumer records available on the black market at 1.4 *billion*[3] - consumers are valuing their own data more and more. A 2016 study by the Ponemon Institute indicated that 75% of respondents stored either a moderate or significant amount of personal data on their mobile phones.[4] Moreover, respondents valued the data on their phones at an average of $14,000, and respondents who took steps to secure the data on their phone valued their data at $16,268.

Surely, the amount of data consumers bring with them every day, and the value they place on that data, has only increased since 2016. And while fraudsters are becoming more sophisticated, the very devices that they seek to penetrate are the devices that have the potential to offer the greatest degree of security when they incorporate MFA 2.0.

[2] https://www.itprotoday.com/identity-management-access-control/security-sense-how-do-you-do-knowledge-based-authentication-when

[3] https://www.pymnts.com/news/security-and-risk/2018/retire-knowledge-based-authentication/

[4]https://www.ponemon.org/local/upload/file/How%20much%20is%20the%20data%20on%20your%20mobile%20device%20worth%20Final%2010.pdf

MFA 2.0's authentication goes far beyond the sophistication with which current hackers and fraudsters operate. By engaging unique, one-time authentication sequencing, efforts to forge, replicate, or guess at an authentication factor stands an exponentially lower chance of success. The ability to pair an identifier such as a highly developed voiceprint, and also the device proximity that MFA 2.0 has the potential to include, means that any individual transaction, as well as overall account security, becomes secure to a degree that the current cybersecurity ecosystem has yet to fully appreciate.

MFA 2.0 Can Support Future Public Policy Challenges

In the coming months and years, "deepfakes" – the use of synthetic audio files derived from actual voice recordings, synced with real (sometimes modified) video, will become a pressing public policy and social issue.[5] While they are currently somewhat rudimentary, increasing sophistication with video and audio development have the potential to wreak havoc with the concept of a democracy based on facts. As this progression occurs, MFA 2.0 will be the single most effective tool to combat these efforts, as it will be able to quickly and accurately determine the authenticity, or lack thereof, of an individual's voice and device origin. Recommended adoption now will help suppress and deter deepfakes in the future.

Next Steps – CCPA and Beyond

The California Attorney General's Office is no stranger to providing guidance on how businesses can best protect themselves and their customers from data breaches. In 2016, this office, under the leadership of then-Attorney General Kamala Harris, issued a data breach report specifically recommending that businesses adopt MFA in order to provide sufficient data security. The report states:

> Th[e] authentication system is failing. We don't use unique passwords for each of our accounts because it would simply be too hard to remember them all...Making matters worse, many individuals do not use strong passwords that are difficult to guess.
>
> A stronger form of online authentication uses multiple factors...this form of authentication should be used by all organizations to help protect access to critical systems and sensitive data. Multi-factor authentication should also be more widely available for consumer-facing online accounts that contain sensitive personal information.[6]

[5] https://www.biometricupdate.com/201902/threat-of-deepfakes-draws-legislator-and-biometrics-industry-attention

[6] https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

The obsolescence of KBA today echoes the report's warnings about weak, commonly-used passwords just three years ago. Instead of weak passwords, KBA's decreasing relevance and inherent weakness derives from easy-to-guess questions and readily attainable information that informs common questions. Attempting to improve KBA by creating more unique or harder questions means these questions will also be harder to remember, and inevitably create greater friction for a customer trying to log on to an app, or interact with a customer-service business function. Even "easy" KBA questions can be difficult to remember – a 2015 study by Google revealed that only 47% of respondents could remember what they put down as their favorite food a year earlier, but that hackers could guess that food (pizza) nearly 20% of the time.[7]

Your office has been charged, in part, to issue rules regarding consumer verification so that businesses can properly identify consumers as they exercise their rights. This presents grave issues of security and authentication. We request that the Attorney General's office issue guidance recommending the use of MFA 2.0, both in this rulemaking and in other forthcoming publications that examine issues of data privacy and security.

It is not a question of whether MFA 2.0 is effective – it is a question of how quickly it will be adopted. California can help chart a course toward the adoption of virtually instant, virtually impenetrable consumer authentication, and we urge the Attorney General to seize this opportunity.

For these reasons, we respectfully request that your verifiable request rules under § 1798.185(a)(7) recommend use of MFA 2.0 as a method to verify requests, and that subsequent cybersecurity guidance do so as well.

Clarissa Cerda

Clarissa Cerda
General Counsel
Pindrop Security, Inc.

[7] https://www.forbes.com/sites/forbestechcouncil/2018/01/22/everybody-knows-how-knowledge-based-authentication-died/#64b13cee4eee

Message

From: Anna Hsia [redacted]
Sent: 12/6/2019 9:54:36 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Proposed Regulations - Comments
Attachments: 191206 California CCPA Reg Comments - ZwillGen.pdf

Attached, please find written comments regarding the proposed CCPA regulations. Thanks in advance for your consideration.

Best,
Anna

ZwillGen

Anna Hsia | Counsel & Head of West Coast Office
369 Pine Street, Suite 506
San Francisco, CA 94104
[redacted]
Bio | Blog | LinkedIn

ZG ZwillGen PLLC 1900 M Street, NW • Suite 250 • Washington, D.C. 20036
(202) 296-3585

Marc J. Zwillinger
[redacted]

December 6, 2019

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

These comments are submitted on behalf of ZwillGen,[1] a law firm that advises hundreds of clients on privacy and security generally and on compliance with the CCPA specifically. The issues identified below reflect the most important changes to incorporate into the final CCPA regulations, as these issues pose specific compliance challenges and/or conflict with the language of the statute. We thank you for considering these comments in their entirety.

Notice of Collection Issue § 999.305(c). The final regulations should clarify the confusion created by the "Notice of Collection" concept in the draft regulations. Section 1798.100(b) of the CCPA requires that: "A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." Until the issuance of the regulations, many businesses presumed that if they collect personal information online, they would satisfy this requirement by providing a link to a privacy policy that described in an accurate and clear way the type of information collected, how it was used, and how consumers could opt out of sales of information. Indeed, such an interpretation would be consistent with the California Online Privacy Protection Act's privacy policy requirements codified at Cal. Bus. & Prof. Code Section 22575 ("CalOPPA"). The Regulations, however, suggest that the notice required by § 100(b) is not the privacy policy itself, but is an additional notice that can be satisfied through a link to the relevant portion of the privacy policy: "If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business's privacy policy that contains the information required in subsection (b)." *See* 999.305(c).[2]

The result of this requirement for websites is that the homepage of the website now has to contain a link to the entire privacy policy as well as a separate "Notice of Collection" link that goes to the relevant portion of the privacy policy (or a separate CA Notice of Collection outside

[1] ZwillGen consists of two entities, ZwillGen PLLC, and ZwillGen Law LLP.

[2] Also see § 999.305(b) describing what the Notice of Collection must contain, including a "A link to the business's privacy policy, or in the case of offline notices, the web address of the business's privacy policy."

of the privacy policy). But it is not quite clear where these links need to be placed. The Notice of Collection provisions of the Regulations require that the Notice be at or before the point of collection, be conspicuous, and:

- Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.
- Be visible or accessible where consumers will see it before any personal information is collected. For example, when a business collects consumers' personal information online, it may conspicuously post a link to the ***notice on the business's website homepage or the mobile application's download page, or on all webpages where personal information is collected.***

The suggestion that the link can be located either on the business's home page, or mobile application download page, or on all webpages where personal information is collected suggests that the link may be placed alongside other required notices—like the Terms of Service or Privacy Policy typically at the bottom of the home page—and not deployed in the form of a banner akin to a pre-emptive European Cookie Banner. When finalizing the Regulations, the AG's office should clarify that placement with these other required notices where consumers know to look for them is acceptable (i.e. consistent with CalOPPA) or specify any other placement that may be required.

Proprietary Data Issue - § 999.313. The Attorney General should make clear in that data ***created about*** consumers by business who have a proprietary interest in such data need not be provided to consumers in response to "Right to Know Requests" seeking specific categories of data. Section 1798.185(a)(3) of the CCPA tasks the Attorney General with authority to establish any exceptions "including, but not limited to, those relating to trade secrets and intellectual property rights." Although such regulations are not required until July 1, 2020, businesses are required to comply with "Right to Know" requests by January 1, 2020, and such requests could implicate information related to consumers that businesses consider to be confidential, proprietary, and/or trade secret information.

Section 1798.100(c)(5) requires businesses to disclose (upon request) "the specific pieces of information that the business has collected about that consumer." But in addition to collecting information directly from the consumer, businesses often generate information related to consumers, including their perceived value to the business, expected profit, costs of acquisition, and expected tenure as a customer. These types of datapoints, while related to an actual consumer, are generated by the business based, in part, on consumer behavior, but are not provided to the business by the consumer or another party. Nor are these business-related data points necessarily about the consumer in the same way that the consumer's contact information or transaction history are. Moreover, they may reveal proprietary business considerations to competitors. We fully expect certain businesses will have employees make Requests to Know of competitors to try to glean understanding of others' business practices from data that would not otherwise be available to them. Because this type of data seems to be outside the intended scope of what needs to be provided back to a consumer upon receipt of an access request, the Attorney General should make clear that valuable proprietary data generated about a consumer by a business need not be provided (at least at this time) in response to an access request, pending more complete regulations issued pursuant to § 1798.185(a)(3). Thus, we propose the following new provision be added as **§ 999.313(12)** on a temporary basis until the AG completes its July 2020 rulemaking.

> **(12)** In responding to a right to know request for specific categories of information, a business need not provide data that is about the consumer but not obtained directly from the consumer or third-parties, provided the business can establish that the disclosure of the information would be valuable to the business' competitors or its disclosure could cause the business financial harm.

Service Provider Exception - § 999.314(c). The Regulations should be broadened to cover the full range of internal operation purposes allowed under the CCPA. The CCPA very specifically recognized that a "business purpose" can include a use "for the business' **or a service provider's operational 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."

The above language thus draws a distinction between the business's and the service provider's operational purposes and indicates there are some permitted "service provider" purposes that are in fact distinct from and not "for the business's . . . operational purposes." Were this not so, the words "or a service provider's operational purposes" would have no purpose in the statute. A fundamental rule of statutory interpretation is "to give meaning to all words used" (*Rodriguez v. Superior Court* (1993) 14 Cal.App.4th 1260, 1269, 18 Cal.Rptr.2d 120) and to avoid "making words surplusage" (*Dyna-Med, Inc. v. Fair Employment Housing Comm'n* (1987) 241 Cal. Rptr. 67, 743 P.2d 1323, 1387). This provision is essential, because it recognizes that service providers can use data from clients to become better service providers—i.e., that their "operational" use of data can align well with their clients' purposes, in many cases.

The Regulations appear to discard this crucial distinction entirely, stating that "a service provider cannot use personal information received from one customer (or from that customer's users) for the purpose of providing services to another person or entity." The Regulations expressly allow service providers to pool personal information across clients solely "to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity." § 999.314(c).[3] This provision unduly limits the purposes in Section 140(d) to a far too narrow set of uses and conflicts with the language of the statute.

In its statement of initial reasons, your Office stated:

> 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

[3] In full, that section reads: "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. A service provider may, however, 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 detect data security incidents, or protect against fraudulent or illegal activity."

> 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.

We think this explanation ignores the reality that providing better service to the business often involves improving the services offered to all of a service provider's customers: indeed we all learn from the information we receive, and build on that information and learning, in providing services to our clients.

> ***Example:*** Assume a service provider is tasked to identify email addresses and physical addresses that are no longer in use for Customer A's large group of brands by scrubbing their lists, and, where necessary, sending marketing communications and removing any bouncing emails from the list and any physical addresses where the mail was marked "return to sender." It keeps an internal "Do Not Mail" list for bad addresses—like fictional ones contained in movies and TV shows. In providing list cleaning services for Customer A, it determines that Joe Smith's email address Joe@joe.com is defunct, and that the street address *1 Main street, Beverly Hills, CA 90210* is a non-existent mailing address, and places them on its internal do not email/mail list. Each time Customer A comes back with a new list for its other brands, the Service Provider removes all defunct email addresses and physical addresses from Customer A's brands by scrubbing them against its internal Do Not mail List. Now Customer B asks the service provider to provide the same cleaning function for its list. The same physical email and address is on Customer's B list, connected with Joe Smith. Must the service provider now repeat the same process from scratch over and over again for all of its customers, on pain of losing its service provider designation? Or can instead use its own Internal Do Not Mail list to remove other incorrect listings.

In the above example, we do not believe the statutory intent is to make the above service provider a "Business"—merely because it uses data across clients to improve its services to all clients. Its data usage is solely to perform a "business purpose" for its customers; Customer A and B have the same business purposes; and there is no further disclosure of Customer A's data to Customer B. Put another way, using data for a common business purpose does not make the use a "commercial purpose."

Accordingly, we would propose the Attorney General withdraw the proposed regulation that prohibits "a service provider's use of personal information collected from one business to provide services to another business," and allow companies to rely on the statutory "reasonably necessary and proportionate" standard. In practice, some services' use of data across clients will fulfill this standard—data hygiene, correction, and validation services come to mind. On the other hand, some services' use of data may not—for instance, the use of data in ways that do not enhance the services provided, or that build data profiles or datasets in ways simply unconnected to the services. Based on many discussions with and among our client base, we believe this distinction is reasonable and intuitive, and standards will readily form as to where the line should be drawn.

Requirements for businesses that do not collect from consumers - § 999.305(d). The Regulations provide two options for a business that does not collect information from consumers to sell the personal information in its possession. Under the Regulations, a business can either:

> (1) Contact the consumer directly to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out in accordance with section 999.306; or
>
> (2) Contact the source of the personal information to:
>
> > a. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b); and
> > b. Obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice.

We believe these options are too limited. Many businesses have personal information under the CCPA (such as Mobile Ad ID, and GPS data) —collected legally and under best practices—yet lack any mechanism to contact the consumer directly. The only option available to such businesses under the Regulations is to confirm that the source provided a notice at collection to the consumer with a corresponding attestation. But this often provides no solution at all: first, such an attestation is unavailable if the data "source" did not interact directly with the consumer, and second, even where an attestation is available, it provides no solution for information collected prior to the time that "notices of collection" existed (i.e., pre-Jan. 1st, 2020). The regulations therefore functionally create a retroactive impact—devaluing legitimate business and data assets, not to mention paid-for contractual expectations—by forbidding the sharing of valid and legally-acquired information.

The Regulations do not, on the other hand, allow for an attestation from someone other than the immediate source of the data, nor do they allow for the use of a data tag, like an icon, flag, or symbol that travels with the data to reflect that proper notice at collection was given. These alternatives would likewise accomplish the same goals while solving the significant operational hurdles identified above. Accordingly, we would recommend the addition that a third and fourth alternative be added:

> (3) Confirm with the immediate source of the personal information that the original source of the personal information has provided a signed attestation describing how the source (a) gave the notice at collection and including an example of the notice or (b) as to personal information acquired prior to the effective date of these Regulations, conspicuously posted a privacy policy in compliance with the California Online Privacy Protection Act. Attestations shall be retained by the business for at least two years and made available to the consumer upon request; or
>
> (4) Verify that the data contains a symbol, icon, or other indication ("Verification Flag") issued by a third-party organization that confirms that the requirements of subsection (a) and (b) have been satisfied, where such third-party organization describes the meaning of the Verification Flag publicly on its website.

Thank you for considering these comments. Please let us know if we can be of further assistance to you during the rulemaking process now or in the future.

Sincerely,

Marc J. Zwillinger
On behalf of ZwillGen PLLC

Anna Hsia
ZwillGen Law LLP

Message

From: Gibbons, Jennifer [redacted]
Sent: 12/6/2019 8:41:30 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Desmond, Edward [redacted]; Sheila Millar, Esq. [redacted]; Leigh Moyers [redacted]
Subject: CCPA Proposed Regulations -- Toy Association Comments December 2019
Attachments: TA Comments to CA AG on Proposed CCPA Regulations fnl 2019-12-06.pdf

Hello,

Attached, please find comments from the Toy Association, on behalf of its members, regarding the proposed regulations related to the California Consumer Privacy Act (CCPA).

By way of background, The Toy Association represents more than 1,100 businesses – toy manufacturers, importers and retailers, as well as toy inventors, designers and testing labs – all involved in bringing safe, fun and educational toys and games for children to market. The Toy Association and its members work with government officials, consumer groups, and industry leaders on ongoing programs to ensure safe play, both online and offline.

The toy industry is deeply committed to privacy, security and product safety, and supports strong and effective standards to protect consumers. We support principles of transparency, notice, consumer choice, access, correction and deletion rights for consumers, and reasonable security, all part of the objectives of the CCPA.

Please feel free to contact us with any questions, or if additional information regarding our comments is needed.

Best,
Jennifer

the toy association

Jennifer Gibbons
Vice President, State Government Affairs

1375 Broadway, Suite 1001 • New York, NY 10018
[redacted] • w. www.toyassociation.org
Follow us on

the toy association

Inspiring Generations of Play

1200 G Street NW • Suite 200 • Washington, DC 20005

[redacted]

December 6, 2019

Via Electronic Submission: privacyregulations@doj.ca.gov

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: Comments on Proposed Regulations Under the CCPA

The Toy Association, Inc. (TTA), on behalf of its members, appreciates the Attorney General's effort to solicit input from stakeholders on the Proposed Text of the California Consumer Privacy Act Regulations (Proposed Regulations) implementing the California Consumer Privacy Act (CCPA) (Cal. Civ. Code §§ 1798.100–1798.199). By way of background, TTA represents more than 1,100 businesses – toy manufacturers, importers and retailers, as well as toy inventors, designers and testing labs – all involved in bringing safe, fun and educational toys and games for children to market. The U.S. toy industry contributes an annual positive economic impact of $109.2 billion to the U.S. economy. TTA and its members work with government officials, consumer groups, and industry leaders on ongoing programs to ensure safe play, both online and offline.

The toy industry is deeply committed to privacy, security and product safety, and supports strong national standards to protect consumers. Our members not only create toys that are physically safe for children to play with, but also engage with children, as well as parents, online. Protecting children and maintaining the trust of parents are the most vital concerns for the toy industry. Likewise, we strongly believe that both safety and privacy should be governed by strong and effective preemptive national laws. Toy industry members are heavily regulated by an extensive set of preemptive laws, including the Children's Online Privacy Protection Act of 1998 (COPPA) (15 U.S.C. §§ 6501–6506), and a variety of product safety laws, such as the Consumer Product Safety Act (CPSA) (codified at 15 U.S.C. §§ 2051-2089) and Federal Hazardous Substances Act (FHSA) (15 U.S.C. §§ 1261-1278), as modified by the Consumer Product Safety Improvement Act (CPSIA). Thus, the toy industry is uniquely qualified to comment on consumer privacy and data security issues raised by these Proposed Regulations, including the important role of preemption, as envisioned by Congress when it enacted COPPA.

Our comments focus principally on inconsistencies between COPPA and the CCPA and Proposed Regulations, as well as the burdens the Proposed Regulations place on both businesses and parents. We do so with a view to offering constructive suggestions on how to align the Proposed Regulations with COPPA. We start with an analysis of the preemptive national framework established by COPPA. COPPA provides broader protections for children, including instances that do not constitute a "sale" under the CCPA. At the same time, as drafted, the Proposed Regulations include elements that are entirely inconsistent with the regulatory framework set forth in COPPA and thus are preempted. Key concerns are:

- CCPA definitions lack adequate clarity that only information collected with actual knowledge that it is from a child is covered. COPPA does not restrict the ability of parents to share their children's information.
- The Proposed Regulations do not account for new methods of verifiable parental consent that might be recognized by the Federal Trade Commission (FTC) under circumstances that may constitute a "sale" under the CCPA.
- As a result of restrictive definitions, the CCPA could restrict activities permitted under COPPA's "support for internal operations" exception.
- COPPA specifies that only parents can make requests to access, update and delete a child's personal information; there is no provision for requests to be made by an "authorized agent."
- Rules regarding access requests for household data could impermissibly violate COPPA.
- COPPA permits, and indeed requires, parents to deny access to children in instances where parental consent is needed and not provided.
- The proscriptive requirements for deleting information, and for receiving and responding to access requests, impose undue burdens on parents and are inconsistent with COPPA.

Finally, we also address considerations related to the opt-in system required for teens (age 13-15) under the CCPA, and offer some observations about the notice obligations outlined in the Proposed Regulations.

I. COPPA Preempts Inconsistent State Law, and the CCPA and Proposed Regulations Recognize Its Preemptive Effect

While many TTA members deal exclusively with parents and adult purchasers, a significant number of our members offer digital experiences directed, primarily or secondarily, to children under 13, so they are keenly aware of their obligations under COPPA. Thus, while our members are affected by the CCPA in all their operations, we highlight some important considerations with regard to the preemptive scheme for a comprehensive national children's privacy law established by Congress more than 20 years ago.

When it enacted COPPA in 1998, Congress recognized the importance of a uniform national preemptive regime governing children's privacy, stating:

> No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.

See 15 U.S.C. §6502(d).

In balancing children's privacy rights with burdens on parents and the need to conduct business operations, Congress, and the FTC, have determined that a wide variety of activities do not require parental consent. For example, COPPA creates a harms-based framework for children's privacy that balances privacy risks to children under 13 for certain types of data collection and sharing with a recognition of business needs and consumer convenience through its definitions, exceptions, and "sliding scale" approach to parental consent. This has worked effectively over the years to safeguard children's privacy.

The CCPA, at §1798.145, recognizes the preemptive effect of some specific federal laws. For example, it confirms that the CCPA does not apply to collection of certain types of information covered by federal law, such as the Health Insurance Portability and [Availability] [sic] Act of 1996 (HIPAA), Gramm-Leach-Bliley, and the Drivers Privacy Protection Act of 1994. The CCPA does not expressly mention COPPA, but §1798.196 contains a general preemption section, stating:

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

The Proposed Regulations appear to acknowledge COPPA's preemptive status, stating that the requirement for obtaining affirmative authorization from a child's parent or guardian for the "sale" of that child's personal information is "in addition to any verifiable parental consent required under [COPPA]." §999.330(a)(1). However, this single reference to COPPA and an attempt to specify in the Proposed Regulations that the CCPA obligations are "supplemental" do not cure potential conflicts with COPPA.

At the outset, it is worth noting that COPPA's protections for children's privacy are broader than those set forth in the CCPA. Under COPPA, for example, any "disclosure" of personal information either collected at a site directed to children or when an operator has actual knowledge that information was collected directly from a child under 13 – regardless of whether there was any exchange of "consideration" for that data - requires verifiable parental consent, unless an exception applies. The statute specifies that parental consent is required in two instances. First, is the "release of personal information collected from a child in identifiable form by an operator for any purpose, except where such information is provided to a person other than the operator who provides support for the internal operations of the website and does not disclose or use that information for any other purposes." Second, is "making personal information collected from a child by a website or online service directed to children or with actual knowledge that such information was collected from a child, publicly available in identifiable form, by any means including by a public posting." 15 U.S.C. § 6501(4).

Even absent an exchange of consideration that would constitute a "sale" as defined by the CCPA, allowing a child to disclose his or her personal information, including by posting selfies or videos, requires verifiable parental consent under COPPA if the information is collected directly from a child. In each case, consent is only required where the information is collected directly from the child, as the statute makes clear. COPPA fully permits parents to post pictures, videos and other information about their children online, including in social media.

Although verifiable parental consent requirements under the CCPA are narrowly focused on a "sale" of personal information with actual knowledge that it was collected from a child under 13, in practice, the CCPA's broad definitions of "personal information" and "sale" pose potential inconsistencies with COPPA. The CCPA's apparent requirement that a business obtain parental consent any time a business engages in the "sale" of "personal information," for example, may conflict with COPPA's exception that permits collection and use of certain information solely to support internal operations. Those arrangements typically do involve a service provider relationship, but that is not a necessary predicate to application of the COPPA exception under the COPPA Rule. Likewise, children may publicly post an "alias" to track and compare game scores anonymously with other users without violating COPPA. Indeed, this is deemed to offer a privacy-safe experience to children that allows them to engage in social interactions without exchanging any "personal" information as defined by COPPA. Because the Proposed Regulations do not address these definitions and inconsistencies, they fail to resolve the tensions between CCPA and the preemptive COPPA regime.

a. Proposed § 999.330 Conflicts with COPPA

The CCPA defines "personal information" at Section 1798.140(o)(1) to include a broad variety of data generally, including data traditionally considered to be anonymous, such as an alias, or an Internet Protocol (IP) address, as well as browsing history. It also includes "household information." Section 1798.140(o)(2) excludes from the broad definition of "personal information" only "publicly available" information. Importantly, and as noted above, COPPA applies only to personal information defined in the statute and COPPA Rule *collected directly from children*, either at a child-directed site or service or where the operator has actual knowledge that it collected personal information from a child under 13. Operators can freely collect and maintain the personal information of children provided by parents or other adults. This happens, for example, when parents, grandparents or others sign up for a gift registry or ask toy brands or retailers for recommendations on age-appropriate toys and games. COPPA imposes no restrictions or obligations in these circumstances.

Section 1798.120(b) of the CCPA implies, similar to COPPA, that the prohibition on a "sale" of personal information of children is linked to instances *where the business has collected the information directly from a child known to be under 13*. The proposed regulations at Section 999.330, however, state that "[a] business that has actual knowledge that it collects or maintains the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child." As drafted, the Proposed Regulation implies a broader restriction that does not square with either the CCPA or COPPA. Any attempted prohibition that would restrict the ability of businesses to freely interface with parents or adults, including obtaining from them information about their children, is inconsistent with and thus preempted by COPPA. A relatively simple solution exists to avoid this conflict: substitute "personal information of children under the age of 13" with "personal information collected from children under 13 with actual knowledge that they are under 13."

Even if that potential inconsistency is resolved as recommended above, the Proposed Regulations present another potential conflict with regard to the enumerated verifiable parental consent methods. The proposed rule at Section 999.330(a)(2) does outline methods recognized under the COPPA Rule as reasonably designed to assure that the individual providing consent is the child's parent or guardian. However, there is one missing element: the COPPA Rule allows authorized safe harbor organizations to approve alternative parental consent mechanisms not enumerated in the Rule. *See* 16 C.F.R. § 312.5(b)(3). To avoid inconsistency, the Proposed Regulations should be modified to automatically recognize other methods recognized by the FTC or by authorized COPPA safe harbor organizations under the process outlined in the COPPA Rule.

b. Allowing Consumer Requests through Authorized Agents Conflict with COPPA

Under the CCPA and Proposed Regulations, a business must honor consumers' requests to access, delete, or opt-out of the "sale" of their personal information made through a properly designated "authorized agent." In contrast, requests to access and delete children's information under COPPA must be submitted by the parent, and the operator must take steps to verify that the requestor *is actually the parent*. This is a direct conflict between COPPA and the CCPA, and the Proposed Regulations do not resolve this conflict.

While the parental authorization process at Section 999.330 does require reasonable steps to determine that the person authorizing a "sale" of personal information is the parent, the Proposed Regulations fail to clarify that under federal law, when it comes to accessing data obtained from children under 13, *a business may only honor requests by a verified parent or guardian*. COPPA makes no accommodation for requests from "authorized agents." The Proposed Regulations further add to the inconsistency with COPPA by requiring that a business receiving an opt-in request from a parent provide the parent notice of the right to opt-out at a later time, as provided under Section 999.315. That section, in turn, specifically allows for such requests to be made by an authorized agent. Additionally, the process for parents to opt-in to sale of a child's information is at odds with the provisions at Section 999.326 which allow an authorized agent to make access or deletion requests. Again, these provisions are inconsistent with COPPA.

Furthermore, the provisions in the Proposed Regulations outlining businesses' duties to respond to requests to know and requests to delete refer to potential conflicts with federal law as a reason to deny a request only as they relate to the requests to know. To clarify the preemptive status of COPPA, and reduce businesses' and consumers' potential confusion regarding their obligations and rights under the CCPA, TTA recommends that the Attorney General revise the Proposed Regulations to specify that all requests to know, delete, and opt into and out of the "sale" of "personal information" as they relate to children under age 13, may only be made directly by a verified parent or guardian, and that an "authorized agent" many not make such requests on behalf of either a child under 13 or a parent of such a child.

c. Right to Request to Know or Delete "Household" Data Conflicts with COPPA

The CCPA instructs the Attorney General to draft regulations to establish rules and procedures for requests pertaining to household information. The Proposed Regulations define a "household" as "a person or group of people occupying a single dwelling." §999.301(h). The Proposed Regulations appear to require businesses to honor requests to know or delete household information if the consumer making the request has a password protected account with the business. Absent a password-protected account, a business may provide aggregate household information, unless all members of the household make the request and the business can individually verify the identity of all members of the household.

These provisions create a potential conflict with COPPA when the household includes children under the age of 13. Where an operator has obtained verifiable parental consent as required under COPPA, the operator likely has "household" information. As noted above, however, if information was collected from a child under 13, the operator must ensure that the requestor is a parent of that child, taking into account available technology, before honoring requests pertaining to the child's information. Under the Proposed Regulations, a consumer with a password-protected account with the business may be able to access a child's information, even if that individual is not that child's parent or guardian. TTA therefore recommends that the Proposed Regulations be revised to clarify that, if a business has household information because initially data was collected from a child under 13, only verified parents or guardians may obtain household information that includes the child's personal information.

d. Non-discrimination Provisions Conflict with Operator Duties under COPPA

Section 1798.125 of the CCPA prohibits discrimination against a consumer who exercises any of the rights set forth in the Act, including "denying goods or services to the consumer," but allows businesses to provide financial incentives to consumers who consent to the collection and sale of their personal information, as long as the incentives are reasonable related to the value of the information.

The Proposed Regulations include detailed rules relating to calculating the value of consumer personal information and disclosures relating to the offering of financial incentives.

These provisions conflict with COPPA. COPPA acknowledges that an operator may terminate a child's access to services if a parent refuses or withdraws consent. 16 C.F.R.§312.6(c). In fact, if services involve, *e.g.*, public disclosure of information, like posting videos or photos, operators subject to COPPA must prohibit the child from accessing the service or feature until parental consent is obtained. To the extent a denial or termination of service to a child could be considered discriminatory under CCPA under these circumstances, it entirely conflicts with COPPA. TTA requests that the Attorney General amend the Proposed Regulations to clarify that a business may deny a child under the age of 13 access to certain services requiring parental consent where the parent does not provide consent under COPPA, and that such denial of service shall not be considered a discriminatory practice under the CCPA.

Finally, we also recommend that the Proposed Regulations clarify that utilization of a credit card with a transaction as a method of verifiable parental consent does not constitute offering a financial incentive under the CCPA.

e. The Proposed Regulations Unnecessarily Increase the Burden on Parents

COPPA requires operators to avoid undue burdens to parents. The Proposed Regulations, in contrast, burden parents as well as businesses. Requests to delete information must involve a two-step process, as do requests to opt-in again to sale of personal information once a parent has opted out. These two-step processes conflict with COPPA's mandate to avoid burdening parents.

The Proposed Regulations set forth proscriptive requirements for businesses to receive and respond to access and deletion requests. A business must provide two or more methods for submitting requests (three if the business primarily interacts with customers in person at a retail location). § 999.312. These methods include at a minimum a toll-free number and a website if the business operates a website or mobile app; businesses may also allow requests to be submitted via email, via an in-person form or a mail-in form. These obligations are inconsistent with and preempted by COPPA, which allows an operator to elect a single method which parents must use to submit a request to access or delete their child's information.

II. Teen Privacy

The Proposed Regulations impose an obligation on a business to obtain "affirmative authorization" before collecting or maintaining any personal information from consumers aged 13-15 that it intends to "sell." The broad definition raises practical considerations. For example, suppose that an online service allows a 13 or 15-year-old to enter a sweepstakes by voluntarily filling out a form, and asks if the registrant would like to receive offers and updates from the third-party company furnishing the prize. This could potentially be deemed to constitute a "sale" under the CCPA. Section 1798.140(t)(2)(A) of the CCPA creates an exception for instances where a consumer uses or directs the business to intentionally disclose the personal information or uses the business to intentionally interact with the third-party, but the inartful wording of the statutory and rule language creates questions about whether this exemption applies where teens are concerned. If this exception does not apply, the Proposed Regulations require that the business must "clearly request" an "opt-in" for "selling" the information and then also ask the teen to "separately confirm their choice to opt-in." The act of filling out a form and checking a box should adequately serve as the affirmative authorization to use the email for the purpose specified and to share it with a third-party.

III. Notices

The detailed requirements for the content of privacy notices outlined in the Proposed Regulations are burdensome for businesses and will likely make it more difficult for consumers to find the information they need. Notably, the Proposed Regulations outline 18 specific items or practices that must be disclosed in a CCPA privacy policy (some of which are redundant). The tension between offering user-friendly privacy polies and prescriptive, specific disclosure obligations is evident in these requirements.

Conclusion

The toy industry is second to none in its support for strong national consumer privacy and safety frameworks. We hope this submittal will assist the Attorney General as it finalizes the regulations under the CCPA. Please contact Ed Desmond at [redacted] or Jennifer Gibbons at [redacted] if you would like additional information on our industry's perspective.

Sincerely,

Steve Pasierb
President & CEO

cc: Sheila A. Millar, Of Counsel

Message

From:	McArthur, Webb [redacted]
Sent:	12/6/2019 4:47:03 PM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC:	Eric Ellman [redacted]
Subject:	CCPA Proposed Regulations Comment Letter - CDIA
Attachments:	CDIA CCPA Proposed Regulations Comment Letter.pdf

Privacy Regulations Coordinator:

On behalf of the Consumer Data Industry Association (CDIA), I submit the attached comment letter regarding the Office of the Attorney General's proposed rulemaking on the California Consumer Privacy Act.

Please do not hesitate to reach out if you have any questions.

Webb McArthur
Associate | Admitted in the District of Columbia, Maryland, and Virginia
Hudson Cook, LLP
[redacted]
1909 K St., NW | 4th Floor | Washington, DC 20006

HUDSON
COOK

The information contained in this transmission may be privileged and may constitute attorney work product. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact Webb McArthur at [redacted] and destroy all copies of the original message and any attachments.

* * * *

CDIA

Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

[redacted]

CDIAONLINE.ORG

December 6, 2019

Via Electronic Delivery to privacyregulations@doj.ca.gov

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: California Consumer Privacy Act Proposed Regulations

The Consumer Data Industry Association submits this comment in response to the California Department of Justice's anticipated rulemaking for the California Consumer Privacy Act ("CCPA").

The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk.

Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs. They help people meet their credit needs. They ease the mortgage and employment processes; they help prevent fraud; they get people into homes, jobs, and cars with quiet efficiency. CDIA members locate crime victims and fugitives; they reunite consumers with lost financial assets; they keep workplaces and apartment buildings safe. CDIA member products are used in more than nine billion transactions each year.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which has been called the original federal consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA"). Accordingly, CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and permissioned use of consumer information is necessary for any CDIA member client to do business effectively.

CDIA members have also complied with an array of state laws for decades, including the California Consumer Credit Reporting Agencies Act ("CCRAA"), the California Investigative Consumer Reporting Agencies Act ("ICRAA"), and the California Commercial Credit Reporting Act.

CDIA appreciates the California Office of the Attorney General ("OAG") for its work on the cutting edge of consumer privacy in the CCPA. It is in this spirit that CDIA offers the following comments to improve the clarity and effectiveness of the proposed CCPA regulations for its intended purposes.

In particular, CDIA has serious concerns about a number of sections of the proposed regulations that, if finalized, would impose requirements and restrictions not provided for in the CCPA. As we describe in greater detail below, these sections do not implement any particular provision in the CCPA and exceed the law's authorization for the OAG to adopt regulations "*necessary* to further the purposes of" the law. *See* Cal. Civ. Code § 1798.185(b)(2) (emphasis added).

Given the specificity contemplated by these proposed regulations and the level of effort proper compliance efforts will take, we respectfully request that the Attorney General provide for an effective date in the final regulations of at least 6 months after publication of the final rule. Businesses will need significant time to develop and implement processes compliant with these requirements.

Furthermore, because of the nature of certain requirements, CDIA respectfully requests that any obligation that is contingent upon the provision of notice prior to taking certain actions either be subject to a later effective date or delayed enforcement date of at 3 months after the effective date for the primary rule. For example, proposed section 999.305(d) requires businesses that do not obtain information directly from consumers to confirm that the source of the information provided a notice at collection in accordance with the regulations (which regulations would have just gone into effect) and obtain signed attestations from sources before selling such information. Without a delayed enforcement date, third party data transfers would halt on the date the regulations are effective.

With regard to the Attorney General's mandate under the law, we believe that adopting regulations with delayed effective and enforcement dates will comply with the directive in section 1798.85(a) of the law.

To assist your office in finalizing regulations that meet consumer expectations and allow businesses to best support customers and consumers, we offer this comment on the proposed CCPA regulations.

We highlight our highest concerns. First, CDIA believes that the OAG exceeds its authority under the CCPA in requiring businesses and service providers to respond to consumer requests relating to personal information exempt from the CCPA, in proposed sections 999.313(c)(5), 999.313(d)(6)(a), and 999.314(d). Where information is not subject to the CCPA sections providing consumer rights, businesses have no obligations relating to those rights under the law.

Second, CDIA believes that the OAG exceeds its authority in restricting the sale of personal information collected from sources other than the consumer in proposed section 999.305(d). The CCPA includes no such restrictions, and the proposed restrictions will cause manifold problems for a range of businesses, as detailed below.

Third, CDIA is concerned that the OAG proposes to require that a business respond to any consumer request, regardless of whether the consumer submitted the request by designated method in proposed section 999.312(f).

And finally, CDIA is concerned that the OAG proposes to limit the use of exempt personal information to uses disclosed to consumers in deletion request responses.

Below we present our comments on the proposed regulation in full.

1. Strike "government entities" from the definition of "categories of sources."

Proposed section 999.301(d) provides a definition for "categories of sources," which must be disclosed in Right to Know requests and in a business' online privacy policy. The proposed definition includes "government entities from which public records are obtained."

ISSUE: Per the 2019 amendments to the CCPA, the term "personal information" does not include "publicly available" information, which includes government records. Because consumers would not receive government records in a Right to Know request, businesses should not be required to disclose that it has received information from government entities from which public records are obtained.

PROPOSED SOLUTION: The phrase "government entities from which public records are obtained" should be stricken from the definition of "categories of sources" at section 999.301(d).

2. Change the term "average consumer" to "typical consumer."

Proposed sections 999.305(a)(2), 999.306(a)(2), 999.307(a)(2), 999.308(a)(2), and 999.315(b) use the term "average consumer." The proposed regulations defined a similar term, "typical consumer," but not "average consumer."

ISSUE: It appears that the term "average consumer" likely has the same meaning as the defined term "typical consumer." However, given that the latter is defined, but not the former, it is not clear what is meant by an "average consumer."

PROPOSED SOLUTION: Change "average consumer" to "typical consumer" to confirm that the OAG means to refer to a "typical consumer."

3. Define the term "disability."

Proposed sections 999.305(a)(2)(d), 999.306(a)(2)(d), 999.307(a)(2)(d), and 999.307(a)(2)(d) require that businesses make notices accessible to consumers with disabilities. However, the term "disability" is not defined.

ISSUE: Given that these required notices are to be presented in writing, either on paper or electronically on a screen, it appears that the disabilities that the regulations seek to address are visual disabilities. But without knowing the meaning of the term, it is impossible for any business to comply with this requirement.

PROPOSED SOLUTION: The OAG should clarify that this requirement is meant to apply specifically to visual disabilities.

4. Remove the requirement to organize the purposes for which personal information will be used by category of personal information in the Notice at Collection.

Proposed section 999.305(b)(2) requires businesses to disclose in a Notice at Collection the business or commercial purposes for which personal information will be used *by category of personal information*. The CCPA, section 1798.100(b), requires disclosure of the purposes for which personal information will be used, but it does not require delineation of purposes by each category of personal information.

ISSUE: The CCPA does not require businesses to provide in a Notice at Collection the purposes for which personal information will be used by each category of personal information. Thus, the OAG exceeds its authority in imposing this requirement.

If this requirement is finalized, businesses might be prohibited from using personal information that the consumer knows the business collected for a purpose for which that the consumer knows the business intends to use their personal information. It is unclear how it furthers the privacy rights of consumers—and the purposes of the CCPA—from preventing businesses from adjusting their business practices when businesses are transparent with consumers about their personal information.

PROPOSED SOLUTION: The OAG should remove the requirement that businesses disclose in a Notice at Collection the purposes for which personal information will be used by each category of personal information.

5. Remove the requirement that businesses obtain "explicit consent" to use personal information for additional purposes.

Proposed section 999.305(a)(3) requires that businesses obtain "explicit consent" (an undefined term) before using personal information for a purpose that was not previously disclosed to the consumer in the Notice at Collection.

ISSUE: The CCPA does not require businesses to provide direct notice and obtain affirmative consent prior to using data for a new purpose. Rather, CCPA section 1798.100(b) provides that "[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section" (emphasis added). The CCPA does not require explicit consent from the consumer.

Further, even if this restriction were permissible and consistent with the purposes of the CCPA, it is not clear how businesses would be expected to comply, particularly for two reasons. First, because this consent requirement relates to the Notice at Collection, which is required for personal information collected directly from consumers. As such, this obligation can only rest on those businesses with a direct relationship with consumers. CDIA members include companies that provide data obtained from sources other than the consumer and do not have direct consumer relationships, and it would not make sense to impose this consent requirement on such businesses. We would encourage the OAG to clarify that this requirement is meant to apply only to personal information collected from consumers.

Second, the term "explicit consent" is not defined, so it is not clear what standard of consent the OAG expects.

PROPOSED SOLUTION: Delete the explicit consent requirement. Businesses are already required to provide notice and make changes to their online privacy policy to account for new uses, and the OAG might impose a 30-day waiting period after an online privacy policy change before new uses would be permitted. Consumers are also empowered to request deletion of data they provide.

6. Eliminate the sale restriction from non-consumer sourced personal information.

Proposed section 999.305(d) prohibits a business from selling personal information collected from parties other than the consumer without either (1) providing a notice that the business sells personal information about the consumer along with a notice of right to opt-out or (2) contacting the source to obtain the notice at collection that was provided to the consumer along with a signed attestation describing how the source gave the notice (along with an example of the notice).

ISSUE: The section 999.305(d) sale restriction is not contained in the CCPA and goes beyond what the OAG is authorized to promulgate. Even if the OAG were authorized by the CCPA to impose this restriction, this subsection seems to contemplate only data sources that collected personal information directly from consumers, not multiple chains of sources. CDIA members may obtain personal information from sources that collected information from a source other than the consumer, and the law does not explain what mid-chain entities must do. CDIA members may also collect a particular piece of information from multiple sources, so it will be impossible to identify one and only one source to locate the correct original Notice at Collection. Businesses generally may not have this level of detail on sources—and no means to contact consumers—and businesses may be contractually prohibited from disclosing their data sources. Finally, it is not clear whether this requirement applies to data exempt from some or all consumer rights under the CCPA.

PROPOSED SOLUTION: Strike this prohibition.

7. Strike "or may in the future sell" in the stated purpose of the Notice at Collection.

Proposed section 999.305(a)(1) provides that the purpose of the notice of right to opt-out of the sale of personal information includes informing consumers of their right to direct a business to refrain from selling personal information in the future.

ISSUE: Section 999.306(a)(1) provides that the purpose of the Notice of Right to Opt-Out relates to personal information that a business "may in the future sell." However, the CCPA—and these proposed regulations—do not require an opt-out notice if a business does not sell personal information. The phrase "or may in the future sell" could be read as requiring all businesses to provide an opt out.

PROPOSED SOLUTION: Strike the parenthetical "or may in the future sell" because it adds confusion to the intent of this section. The phrase "business that sells" is broad enough to cover a business that may sell personal information later in time.

8. Strike the requirement to provide an offline notice of right to opt-out.

Proposed section 999.306(b)(2) provides that a business that substantially interacts with consumers offline must provide a notice of right to opt-out by offline method. The CCPA does not, in any place, require such a notice to be made offline.

ISSUE: The text of the CCPA does not require a business to provide a Notice of Right to Opt-Out offline, so the OAG is not authorized to impose a notice requirement that the law does not contemplate.

Even if the OAG were authorized to require this, the term "substantially" in section 999.306(b)(2) is not defined, and it is impossible to know whether a business has complied with this requirement. Additionally, it is not clear what interactions would qualify as "offline" interactions, but it appears that the term "offline" is meant to target in person interactions.

PROPOSED SOLUTION: Strike this requirement or, alternatively, change the terms "substantially" to "primarily" and "offline" to "in person."

9. Strike the requirement that a business without a website provide a notice of right to opt-out.

Proposed section 999.306(b)(3) provides that a business that does not operate a website must notify consumers of their opt-out right by another method. The CCPA does not, in any place, require any notice of right to opt-out be made in any place other than online.

ISSUE: The text of the CCPA does not require a business to provide a Notice of Right to Opt-Out if it does not operate a website, so the OAG is not authorized to impose a notice requirement that the law does not contemplate.

PROPOSED SOLUTION: Strike this requirement.

10. Provide for flexibility in presenting the notice of right to opt-out.

Proposed section 999.306(c) details all of the information that must be included in the notice of right to opt-out, including directing consumers to the business' privacy policy.

ISSUE: The level of detail required in the notice of right to opt-out will likely overwhelm the typical consumer and frustrate business' efforts to present the notice in a way that is easy to read and understandable by a typical consumer, as is required by proposed section 999.306(a)(2), as well as businesses' efforts to educate effectively consumers about opting out.

PROPOSED SOLUTION: The OAG should allow for flexibility in presenting the notice of right to opt-out.

11. Remove the requirement that a business commit not to sell personal information in the future.

Proposed section 999.306(d)(2) provides that a business is not required to (1) provide a notice of right to opt-out of the sale of personal information if it does not, and will not, sell personal information during the period which the notice of right to opt-out is collected and (2) the business states in its privacy policy that it does not, and will not, sell personal information.

ISSUE: Businesses may decide to sell personal information when they previously had not. If finalized, this provision would require businesses to commit not to sell personal information on consumers in the future, effectively tying their hands in making business decisions because they decided not to publish notice of a right to consumers that was not, in fact, even available with consumers.

Businesses should be required to provide opt-out rights—and the notice of right to opt-out—when the business sells personal information on consumers. But businesses should not be required to commit to future business practices in order to avoid deceiving consumers.

PROPOSED SOLUTION: The OAG should strike the requirement to commit to not sell personal information in the future and the requirement to provide notice in an online privacy policy that the business will not sell personal information in the future. In its place, the OAG can clarify that businesses are required to provide notice of right to opt-out before it first sells personal information on consumers.

12. Strike the requirement that businesses consider consumers to have opted out when a business does not provide a notice of right to opt-out.

Proposed section 999.306(d)(2) prohibits a business from selling personal information to third parties that it collected at a time at which it did not sell personal information to third parties and did not provide for a notice of right to opt-out.

ISSUE: See comments to proposed section 999.305(a)(3) above. By deeming such consumers as "opted out," this proposed regulation could be read to require affirmative consent prior to sale, which goes beyond what is required in the CCPA. The CCPA requires that consumer be provided notice as required by the CCPA prior to any new use or sale; the CCPA does not prohibit businesses from selling personal information on consumers without getting the consumers' affirmative consent.

Additionally, opting consumers out of sale without providing them the notices required by the CCPA may be contrary to consumer choice and would be contrary to the purpose of the law, which is to give consumers rights to control their personal information. Any business selling personal information to third parties must provide the "Do Not Sell" button and an opt-out mechanism. Consumers wishing to be opted out of sale would be permitted to exercise these rights when there is any right to exercise.

PROPOSED SOLUTION: Strike this requirement. The sale restriction is beyond what the OAG is permitted to require in these regulations. The CCPA already requires that consumers be notified of their right to opt-out where it is applicable, but the OAG might impose a 30-day waiting period after publication of a notice of right to opt-out before a business is permitted to sell personal information.

Alternatively, add "required but" after "notice of right to opt-out notice is" in proposed section 999.306(d)(2) to clarify that the opt-in requirement would apply only where a business was required to provide notice of right to opt-out and did not do so.

13. Strike the requirement that businesses must describe the method by which businesses calculated the value of consumer's data.

Proposed section 999.307(b)(5)(b) requires that a business offering differential prices or services to provide a notice of financial incentive, which must include a description of the method by which the business calculated the value of the consumer's data.

ISSUE: Proposed section 999.337 gives businesses broad discretion in valuing consumer data for the purpose of offering a permitted differential price or services. Therefore, the exact formula by which a business may determine the value of consumer data may be trade secret information to the business. The OAG should not require the disclosure of trade secrets.

PROPOSED SOLUTION: Strike this requirement.

14. Strike the requirement to disclose privacy policy information by category of personal information.

Proposed section 999.308(b)(1)(d)(2) requires businesses to disclose in their privacy policy the categories of sources of personal information, the business and commercial purposes for using personal information, and the categories of third parties to whom personal information is sold, each organized by the category of personal information collected. The CCPA does not require this information to be disclosed by each category of personal information in an online privacy policy.

ISSUE: The required disclosure of the categories of sources, business and commercial purposes, and categories of third parties *organized by category of personal information* will be difficult, if not impossible, to comply with for many businesses. Businesses may not have historically tracked information to this level of detail, which requires grouping these items by categories that were created in the CCPA (in the definition of "personal information"). Additionally, businesses may have collected the same information from multiple sources, requiring businesses to separate out multiple copies of the same information in order to describe sources, which could make the disclosure cumbersome and confusing to consumers. The text of the CCPA also does not require disclosure of this level of detail of information about sources, purposes, and third parties receiving personal information in an online privacy policy.

PROPOSED SOLUTION: Strike the requirement that the categories of sources, business and commercial purposes, and categories of third parties to whom business shared personal information *by category of personal information* in online privacy policies, instead permitting disclosure of each of the sets of information generally.

15. Strike the requirement that businesses state whether or not it sells personal information of minors under 16 years of age without affirmative consent.

Proposed section 999.308(b)(1)(e)(3) requires businesses to state, in their online privacy policy, whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization. CCPA section 1798.120(c) prohibits businesses from selling the personal information of consumers under 16 years of age without affirmative consent.

ISSUE: The requirement to state whether the business sells personal information on minors under 16 years of age without affirmative consent is not necessary because the law does not permit such sale. It would also require a business violating the law to state that it is violating the law or risk incurring a second violation for each violation of the minor sale restriction.

PROPOSED SOLUTION: Strike this disclosure requirement.

16. **Correct business' requirement to describe consumers' right to delete.**

Proposed section 999.308(b)(2)(a) requires businesses to explain, in their online privacy policy, that a consumer has the right to request the deletion of their personal information maintained by the business. CCPA section 1798.105(a) provides that consumers have the right to request a business delete any personal information about the consumer which the business has collected from the consumer. This right under the law does not extend to any information *maintained* by the business (notably, information collected from sources other than the consumer).

ISSUE: This section provides that businesses must explain that consumers have the right to request deletion of personal information maintained by the business, but the CCPA only provides this right for personal information that the business *collected from the consumer*. Consumers have no right, under the law, to request deletion of personal information a business collected from a source other than the consumer. To require businesses to describe consumers' right in this way would risk confusion of consumers as to their rights under the CCPA.

PROPOSED SOLUTION: Strike the words "or maintained."

17. **Clarify that businesses are only required to explain consumer rights to the extent they are available with the business.**

Proposed section 999.308 requires a business to disclose, in a business' online privacy policy, that consumers have various rights under the CCPA (The Right to Know about Personal Information Collected, Disclosed, or Sold; the Right to Request Deletion of Personal Information; and the Right to Opt-Out of the Sale of Personal Information). However, businesses are not required to comply with the CCPA for a number of types of personal information, as set out in CCPA section 1798.145.

ISSUE: Section 999.308 requires disclosure of CCPA consumer rights (The Right to Know about Personal Information Collected, Disclosed, or Sold; the Right to Request Deletion of Personal Information; and the Right to Opt-Out of the Sale of Personal Information), but it does not specify that businesses are required to comply with these disclosure requirements only to the extent that the particular rights are actually applicable to personal information held by a business. The CCPA exempts certain sets of personal information from many, if not all, consumer rights, and it would be contrary to the purposes of the law—and would create confusion—to require businesses to advise consumers on consumer rights that do not exist with the business. For example, the activities of consumer reporting agencies largely fall within the FCRA exemption, so it would add confusion to require the business to tell consumers that they have rights that they, in fact, do not have.

PROPOSED SOLUTION: Section 999.308 should be amended to explain that businesses must provide notice of consumer rights under the CCPA only where such consumer rights may be exercised with respect to personal information held by such business.

18. **Correct designated consumer requests method requirements based on current law.**

Proposed section 999.312(a) requires businesses to provide two or more designated methods for submitting requests to know. The CCPA was amended in 2019 to provide that businesses that operate exclusively online and have direct relationships with consumers from whom they collect personal information are only required to provide an email address for submitting Right to Know requests.

ISSUE: As drafted, this proposed regulation section conflicts with the CCPA.

PROPOSED SOLUTION: Amend this requirement consistent with the 2019 changes to the law.

19. Remove the requirement for a business to respond to a consumer request submitted by a non-designated method.

Proposed section 999.312(f) requires that a business in receipt of a Right to Know or deletion request submitted by a method other than one of its designated methods of submission must either treat the request as if it had been submitted in accordance with a designated method or provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable.

ISSUE: The CCPA does not require businesses to accept or redirect a request made to a business by any method. Section 1798.130(a)(1) of the CCPA requires businesses to establish one or two designated methods, depending on the way in which the business interacts with consumers. Therefore, the OAG exceeds its authority in requiring businesses to respond to a request submitted by any method.

This requirement will expose businesses to disclosing personal information to fraudulent or abusive sources that may send mass requests to businesses, not through designated channels, such as abusive credit repair clinics. It would also require businesses to train all employees and contractors in dealing with consumer requests, even those that have no consumer-facing functions. Finally, this requirement would prove difficult to manage, considering an infinite number of avenues in which consumers might attempt to contact a business to lodge a request.

Consumers will be provided one or two methods by which they can submit requests. Businesses will have to explain these methods in the business' online privacy policy.

PROPOSED SOLUTION: Remove the section 999.312(f) requirement that a business respond to consumer requests submitted by non-designated methods.

20. Limit the requirement to disclose categories of personal information only where the consumer requests that information.

Proposed section 999.313(c)(1) provides that if a business cannot verify a consumer as to a request to know the specific pieces of personal information about a consumer, it must consider whether it can verify the consumer as if the consumer was seeking the *categories* of personal information about the consumer.

ISSUE: The CCPA does not require businesses to provide information in a Right to Know request that the consumer has not requested. Specifically, the law does not require businesses to provide the categories of personal information about a consumer when the consumer requests the specific pieces of information. As a result, the OAG attempts to exceed its directive under the CCPA in imposing this requirement. Businesses should not be required to provide information that a consumer does not request in response to a Right to Know request.

PROPOSED SOLUTION: Amend this requirement to apply only where the consumer specifically requests categories of personal information in addition to the specific pieces of information.

21. Strike the requirement that a business respond to a request relating to exempt personal information.

Proposed section 999.313(c)(5) requires that if a business that denies a consumer request to know on the basis of an exemption under the law, it must inform the requestor and explain the basis for the denial.

ISSUE: The CCPA's various exceptions provide that the certain kinds of personal information are exempt from most, if not all, of the requirements of the CCPA, including the CCPA's right to know. Therefore, the OAG is not authorized under the CCPA to require businesses that are exempt from the CCPA to comply with CCPA obligations, including responding in a particular way to consumer requests.

PROPOSED SOLUTION: Eliminate requirement that a business must respond to a consumer making a Right to Know request relating to exempt personal information.

22. Strike the requirement to disclose information in a Right to Know request by category of personal information.

Proposed section 999.313(c)(10) requires businesses to disclose, following a verified Right to Know request, the categories of sources of personal information, the business and commercial purposes for using personal information, and the categories of third parties to whom personal information is sold, each organized by the category of personal information collected. The CCPA does not require this information to be disclosed by each category of person information.

ISSUE: The required disclosure of the categories of sources, business and commercial purposes, and categories of third parties *organized by category of personal information* will be difficult, if not impossible, to comply with for many businesses. Businesses may not have historically tracked information to this level of detail, which requires grouping these items by categories that were created in the CCPA (in the definition of "personal information"). The text of the CCPA also does not require disclosure of this level of detail of information about sources, purposes, and third parties receiving personal information.

PROPOSED SOLUTION: Strike the requirement that the categories of sources, business and commercial purposes, and categories of third parties to whom business shared personal information *by category of personal information*, instead permitting disclosure of each of the sets of information generally.

23. Remove the requirement to treat a deletion request as an opt-out request.

Proposed section 999.313(d)(1) requires that a business that cannot verify the identity of a consumer for a deletion request to treat the request as a request to opt-out of the sale of personal information to third parties. The CCPA requires businesses to honor a consumer's deletion request and a consumer's opt out request, but it does not, in any place, require a business to provide an automatic opt out to a consumer making a deletion request.

ISSUE: The law does not require that a business opt a consumer out of sale if they cannot be verified for a deletion request.

PROPOSED SOLUTION: Remove the requirement to opt the consumer out of sale when a deletion request cannot be verified. Consumers individually have the right to request opt out. The OAG could require that businesses declining to honor a request on the basis of being unable to verify the identity of the consumer must inform consumers of other rights under the CCPA.

24. Clarify the allowance regarding the deletion of archived information.

Proposed section 999.313(d)(3) permits a business to delay deletion of personal information, as requested by a consumer, maintained on archived or backup systems until the system is next accessed or used.

ISSUE: Businesses may access archived databases regularly, but with a set purge schedule. Businesses should not be required to effectuate all pending deletion requests any time it connects to a database for any purpose.

PROPOSED SOLUTION: Permit deletion to be made in archived databases "in the normal course of business so long as the personal information is not sold."

25. Remove the requirement that a business respond to a deletion request for exempt personal information.

Proposed section 999.313(d)(6)(a) requires a business that denies a consumer's deletion request on the basis of an exemption under the CCPA to inform the consumer that it will not comply with the request and explain the basis for the denial. CCPA section 1798.145 provides that the CCPA does not apply, at all, to various types of personal information.

ISSUE: The CCPA's various exceptions provide that the certain kinds of personal information are not subject to the CCPA. Therefore, the OAG is not authorized under the CCPA to require businesses that are exempt from the CCPA to comply with CCPA obligations, including responding in a particular way to consumer requests.

PROPOSED SOLUTION: Eliminate requirement that a business must respond to a deletion request relating to exempt personal information.

26. Permit businesses to use information that it declined to delete for any exempt use.

Proposed section 999.313(d)(6)(c) prohibits a business that denies a consumer deletion request on the basis of a particular exception under the CCPA from using that personal information for a purpose other than was previously described in a denial to a deletion request. The CCPA does not restrict a business from using personal information in a particular way where it, at any point, had previously used the information for a purpose exempt from the law. CCPA section 1798.145 provides that the CCPA does not apply, at all, to various types of personal information.

ISSUE: The CCPA provides multiple exceptions from its scope. A business may be eligible for a particular exemption and deny a consumer request based on that exemption. However, at a later time, a business may want to use the same information for a use contemplated under a separate exemption, and the CCPA does not prohibit a business from relying on a separate exception that may not have been applicable when the business rightfully declined a consumer request. This defeats the purpose of each of these exemptions, frustrates compliance with federal law, and is contrary to the purposes of the law.

PROPOSED SOLUTION: Add "or any other exception or permitted use" to the end of section 999.313(d)(6)(c).

27. Expand express permissions for service providers.

Proposed section 999.314(c) prohibits a service provider from using personal information it received in its capacity as a service provider to a particular business for the purpose of providing services to another person or entity, except that it may combine personal information from multiple engagements to detect data security incidents or to protect against fraudulent or illegal activity. The CCPA does not prohibit service providers from using personal information in a way that is contractually authorized by their client business.

ISSUE: Many businesses, including CDIA members, may act as service providers and may engage other service providers as sub-contractors. Businesses may also "white-label" products to multiple clients as a service provider, which may involve providing certain personal information to multiple clients for the same product or combining information from multiple clients to service the white-labeled product. As written, it is not clear that this section 999.314(c) requirement would permit businesses to continue to sub-contract or white-label their products. Additionally, businesses should be permitted to combine personal information from multiple businesses for analytical purposes (for example, to compare a company's customer base to industry- and geography-wide numbers).

PROPOSED SOLUTION: Add explicit authorization to share personal information to another service provider (with appropriate contractual restrictions), to another business in delivering a set product of service of the service provider (white-labeling), and to provide analytical services.

28. Strike the requirement that service providers respond to consumer requests.

Proposed section 999.314(d) requires service providers receiving and denying a consumer request under the CCPA to explain the basis for the denial of the request and inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information. The CCPA does not impose any disclosure requirement on service providers.

ISSUE: The CCPA does not impose requirements relating to consumer rights on service providers, as opposed to businesses. These service providers, which include CDIA members, do not obtain personal information for commercial gain from the data, and they are not in the best position to provide any information on consumers or verify the identity of consumers, since service providers are unlikely to have direct relationships with consumers. Finally, service providers may not be permitted to disclose the identity of their clients.

PROPOSED SOLUTION: Eliminate the requirement that service providers must respond to consumer requests.

29. Strike the requirement that businesses treat user-enabled privacy controls as opt-out requests.

Proposed section 999.315(c) requires that businesses treat user-enabled privacy controls that communicate or signal a consumer's choice to opt out of the sale of their personal information to third parties as a valid request to opt out for that browser or device or, if known, for the consumer. The CCPA protects "personal information," which is, per CCPA section 1798.140(o)(1), information that reasonably may be linkable to a particular individual or household, not merely a device.

ISSUE: The CCPA does not protect information that cannot reasonably be linked to a particular person or household, whether or not the business can detect that information relates to a particular device. This requirement is therefore beyond the scope of the CCPA and the OAG exceeds its authority under the law in attempting to impose this requirement.

To the extent that information may reasonably be linked to a particular consumer or household, consumers can install browser privacy controls for a variety of reasons, many of which do not equate to desiring for their information not to be sold to third parties. The CCPA does not provide for a right to be opted out from the sale of personal information by installing any browser privacy control. Furthermore, this technology is evolving and there will likely be compatibility problems with these controls.

PROPOSED SOLUTION: Eliminate the requirement that user-enabled privacy controls be treated as opt-out requests.

30. Simplify timing requirements for opt-out requests.

Proposed section 999.315(e) requires businesses that receive an opt-out request to "act upon" the request within 15 days from the date the business receives the request.

ISSUE: The term "act upon" is not defined, so it is not clear what the business must have completed within 15 days of receiving the request. Many businesses, including CDIA clients, have data transfer cadences that are quarterly or monthly, but this requirement would require all businesses to increase their transfer cadences to multiple times a month to capture all requests within this proposed timeline.

PROPOSED SOLUTION: Simplify the timing requirement to completing the request in 45 days, which is consistent with other consumer rights under the law.

31. Delete the requirement that a business notify third parties to whom it sold personal information after an opt-out request.

Proposed section 999.315(f) requires a business honoring an opt out request to notify all third parties to whom it had sold the personal information within the last 90 days and instruct those third parties not to further sell the information. The CCPA does not impose any third party notification requirement, nor does it impose any requirement for a third party to honor a consumer's opt out request made to another entity.

ISSUE: The statute does not obligate businesses to notify third parties to which it sold personal information upon a consumer's opt-out request. Therefore, the OAG does not have the authority under the law to require this. Furthermore, these businesses may not be in an ongoing contractual relationship that would allow one business to prevent the other from further selling the information.

Consumers may also not want to opt out of the sale of personal information to all businesses. Finally, complying with this requirement would require businesses to exchange personal information, which is contrary to the purposes of the law and could increase the incidence of identity theft.

PROPOSED SOLUTION: Delete this section 999.315(f) requirement. Consumers will already have the right to opt-out of sale with any business.

32. Clarify that businesses may request additional information from the requestor for matching purposes.

Proposed section 999.315(h) provides that an opt out request "need not be a verifiable consumer request" and that a business may decline to honor such a request if it believes the request is fraudulent.

ISSUE: Even though businesses are not required to utilize any particular verification process for opt out requests, businesses will need to be able to match a requestor to the personal information of a particular consumer. In that light, this proposed section does not explicitly permit a business to request additional information a business may need to match the requestor with a consumer in the business records or to decline a request if a consumer has not provided adequate information. This will be a particular problem for consumers with common names. Additionally, this section does not provide an explicit basis to deny a request if a business cannot definitely match the requestor with a consumer in its records.

PROPOSED SOLUTION: The OAG should clarify that businesses may request additional information from the requestor to match them to a consumer in the business' records. Additionally, the OAG should clarify that a business can decline to honor an opt-out request if, after attempting to match the requestor, the business is unable to match the requestor with a consumer in its records.

33. Remove the recordkeeping metrics requirements.

Proposed section 999.317(g) requires businesses to compile and disclose various metrics about their CCPA compliance. The CCPA does not require businesses to make such calculations or disclose any of this information.

ISSUE: These recordkeeping requirements appear nowhere in the CCPA. The OAG exceeds its authority in imposing these calculation and disclosure requirements.

Additionally, it is not clear whether these requirements apply to personal information exempt from the CCPA.

PROPOSED SOLUTION: The OAG should remove these calculation and disclosure requirements.

34. Eliminate the requirements relating to honoring individual requests for household information.

Proposed section 999.318(b) requires businesses that receive and can individually verify a request of all members of a household to honor such consumers' request with regard to household information. The CCPA does not contemplate a business being required to honor multiple consumers requests collectively.

ISSUE: This section 999.318(b) requirement is problematic because it risks breaching the privacy rights of individuals without adding any benefit to involved consumers. Businesses will not be in any position to determine whether all individuals that submit a request are all members of the household. As a result, a business may disclose personal information on individuals without permission, which will increase the incidence of identity theft. This requirement does not provide any rights that consumers do not otherwise have under the CCPA, as consumers can individually request information on them.

PROPOSED SOLUTION: Eliminate this section in its entirety. Consumers have the ability to request personal information on them.

35. Strike the general data security requirement.

Proposed section 999.323(d) seeks to impose certain general data security measures on regulated businesses.

ISSUE: The CCPA does not impose a general data security requirement, but instead provides for certain defenses to private suits in the event of a breach that results from a business's "violation of the duty to implement and maintain reasonable security procedures and practices." Further, even the law could be read as imposing an affirmative obligation, proposed section 999.323(d) does not mirror the language of the law but goes beyond it. Section 1798.150(a) applies to "unauthorized access and exfiltration, theft, or disclosure," and does not provide for a suit if information is deleted. There is no duty to prevent deletion of a consumer's personal information in the law.

PROPOSED SOLUTION: Delete this provision.

* * *

CDIA thanks the California Department of Justice for the opportunity to share its views on the proposed CCPA regulations. Please contact us if you have any questions concerning the above comments or need additional information.

Sincerely,

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs

Message

From: Fatima Khan [redacted]
Sent: 12/6/2019 10:13:27 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Proposed Regulations Comments
Attachments: Okta_PublicComment_CCPA_12.6.19_final.pdf

Hi –

Please see the attached document for Okta's comments. Thank you for your consideration.

Best,
Fatima

December 6, 2019

The Honorable Xavier Becerra
California Attorney General
California Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Via E-mail: privacyregulations@doj.ca.gov

Re: California Attorney General – California Consumer Privacy Act of 2018: Proposed Regulations
Comments of Okta, Inc.

Dear Mr. Attorney General Becerra:

Okta, Inc. ("Okta") appreciates the opportunity to provide these comments in connection with the California Attorney General's ("AG") proposed regulations for the California Consumer Privacy Act of 2018 ("CCPA").

Okta Overview

Okta is a publicly-traded (NASDAQ: OKTA) cloud computing company that offers identity and access management software-as-a-service to businesses, governments, non-profit entities, and other organizations across the United States and around the world. Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables the company's customers to securely connect people to technology, anywhere, anytime and from any device. The company was incorporated in January 2009 as Saasure Inc., a California corporation, and was later reincorporated in April 2010 under the name Okta, Inc. as a Delaware corporation. Okta is headquartered in San Francisco, California.

Okta's customers use our services to work with some of their mission-critical, sensitive data, including the names, email addresses, and mobile phone numbers of their users. As a growth company, Okta continues to surpass key milestones: just recently, we cleared the 100 million user mark[1]. Accordingly, acting with integrity and transparency, so that we earn and maintain our customers' trust, is critically important to all of us at Okta. To that end, Okta maintains privacy protections across its suite of services, as detailed in our third-party audit reports and standards certifications.

Although many companies may view privacy compliance as a burden, Okta views it as a strategic differentiator and a competitive advantage — we provide tools and resources to our customers, to help ensure that their own systems are kept safe and secure, so that critical data can remain private and protected.

For these reasons, Okta commends California's current work towards implementing a comprehensive privacy law with the hope that such law protects consumers and enables businesses to strengthen their approach to privacy through clear compliance obligations. Okta's approach to privacy aligns with the CCPA, including support for the view that "it is possible for businesses both to respect consumers' privacy and provide a high level transparency to their business practices."[2]

Introduction

Okta agrees with the AG's sentiments that today more than ever, strong privacy and security programs are essential to the people of California and our economy.[3] As technology advances, California is continuously the leader at the forefront of protecting the privacy and security of consumers, and Okta supports the state's efforts. In addition to being a trailblazer in protecting consumer privacy, Okta also encourages the state of California and the AG to remain engaged with both federal and other states' efforts to further privacy protection in order to create regulation and guidance that will best allow companies to strengthen privacy practices for consumers.

Furthermore, Okta encourages California to continue to advance consumer privacy through risk-based, flexible privacy regulation that provides clear compliance obligations for businesses. We believe that being unduly prescriptive can result in stifling compliance checklists that inhibit the creation of innovative privacy solutions or frustrate consumer privacy efforts due to implementation hurdles. Benefits should be measurable and quantifiable, and any new state privacy legislation should first take into account the outcomes sought by consumers, and also align with California residents' understanding of meaningful data protection.

Key Points for Consideration

We offer three key areas for consideration as part of the AG's analysis on updating the proposed California Consumer Privacy Act Regulations ("Proposed Regulations").

First, it is important that the AG account for the complexity of technology and the different scenarios that arise through the use of personal information. Although Okta is aware of the risks associated with processing personal information, there are instances when consumers may prefer to share their personal information with companies that are best positioned to protect consumer privacy and security through their services. As follows, it is important to ensure that the CCPA accounts for different business models and enables the use of personal information for purposes compatible with providing services to further innovation and to consistently improve upon pro-privacy and security technologies.

Second, as a service provider to our customers, Okta has core values to "love our customers" and "act with integrity." In line with these values, Okta wants to make sure that it honors these promises to its customers and acts with integrity by respecting the confidentiality and security safeguards in place with regards to the personal information our customers entrust to us for our services. As a service provider, Okta cannot interfere with its customers' direct relationships with consumers due to its obligations to honor its contracts and maintain reasonable security. As follows, Okta encourages the AG to clearly delineate responsibilities with regards to individual rights requests, such as to know or delete, to ensure that these responsibilities fall on businesses to carry out as the party with the direct relationship and limit the service provider's role in responding to such requests.

Third, Okta believes that the CCPA would benefit from clarification and alignment with existing global and federal privacy and security standards around identity, to ensure that proper identity verification is in place for consumer privacy rights requests. In line with these global standards, Okta encourages the AG add in a clarification to require businesses to use multi-factor authentication (MFA), when possible, for satisfying requests to know or delete to prevent the abuse of privacy rights and to ensure personal information is only furnished to individuals upon a properly verified request.

1. Request for the clarification of section 999.314(c) of the Proposed Regulations to permit the use of personal information by a service provider for compatible purposes.

As stated in the CCPA, "it is almost impossible" to conduct even the most mundane tasks without sharing personal information.[4] Based on the pervasive need to collect personal information to carry out even the most simple technical tasks, it is important for the state of California to account for the wide array of business models that need to collect personal information to carry out the services they provide to consumers and to businesses. Okta does not monetize personal information, but provides a cloud-based enterprise solution that helps to streamline identity management and increase efficiencies for companies and their end users to securely access cloud-based applications.

The text of the Proposed Regulations, Section 999.314(c) states that 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."

However, "[a] service provider may . . . combine personal information received from one or more entities . . . on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity."

The Proposed Regulations should elaborate upon the key distinction between (i) commercialization of personal information and (ii) the internal use of personal information to further the provision of services to businesses and maintaining service providers' ability to innovate on their services provided using such personal information. Some examples of these use cases include: (i) aggregating and analyzing personal information in line with contractual requests made by customers to do so; (ii) providing and improving upon the services requested by businesses in contracts; (iii) gathering statistical research data to provide de-identified benchmarking and trends to businesses; and (iv) innovation that helps create a more privacy-forward and secure Internet for businesses and consumers, such as through the use of large data sets to power artificial intelligence algorithms for the benefit of all.

In harmony with use cases found across existing California law [5] and global legal frameworks [6], Okta requests the clarification of section 999.314(c) of the Proposed Regulations to permit service providers to use personal information for reasonable compatible purposes. Such a clarification is consistent with the use cases defined within the definition of "business purpose" in section 1798.140(d) which states "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*" including "performing services on behalf of the business or service provider" as described in section 1798.140(d)(5) (emphasis added).

Furthermore, the ability for service providers to utilize personal information would also fall within the scope of the "reasonably necessary and proportionate" standard described in section 999.314 of the Initial Statement of Reasons [7]. For cloud-based enterprise companies that do not monetize personal information, including those in the identity and security space, a clarification that such use of personal information is permitted to better innovate on their services for their customers to receive a more secure and usable solution would result in a safer Internet for all users.

Okta supports the California legislature's key drivers for the service provider limitations and we believe that a uniformly applied set of reasonable and legitimate personal information use rights for service providers can help achieve those goals. Therefore, any privacy regulation should include terms that permit companies to achieve compliance and innovate to create a better services for their customers, thereby resulting in a more secure Internet for all users in line with smooth interoperability between the existing state laws, the U.S. privacy landscape, and privacy regulations in other countries.

2. Request for the clear delineation between service provider and business requirements with regards to individual requests to know or to delete personal information.

Consistent with the CCPA's key distinction between service providers and businesses, we request a clear delineation on each party's respective obligations with regards to completing individual rights requests to know or to delete personal information. At present, section 999.314(d) states:

> 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 does not comply with the request, it shall explain the basis for the denial. The 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.

As required of service providers under the CCPA, Okta has in place specific contractual restrictions to limit the use, disclosure, and access to the personal information entrusted to us by customers for our service. Since businesses engage service providers like Okta with their personal information to provide services, not communicate independently with their consumers, the obligations in section 999.314 put service providers at odds with their obligations to customers and may adversely impact the reasonable security measures and access management safeguards that service providers have in place to protect their customers' personal information.

While the text of the CCPA makes clear that businesses have an obligation to carry out these requests, the Proposed Regulations include the addition of an obligation on service providers to handle such requests by sharing details directly with the consumer as well as potentially requiring service providers to access or delete personal information in its possession. As a result of this tension, the service provider faces conflicting obligations through the law and its contracts and would potentially have a legal obligation to access personal information to satisfy a consumer request that is normally protected by contractual and security safeguards, such as access controls. For example, as a service provider, Okta may hold personal information separately for different customers and would not know which business is relevant to a consumer's individual request unless informed by the consumer. To access such information, Okta would have to bypass normal security safeguards and access controls across its customers to be able to provide an appropriate response. This in turn, would diminish an individual's security and privacy as well as put similarly situated companies in direct conflict with their contractual obligations and company values.

Furthermore, the lack of clarity around responsibility and accountability for carrying out privacy requests by consumers could result in consumer confusion and request fatigue. The consumer should have a single dedicated channel for any requests arising out of the original data collection by the business with corresponding accountability for the business. To mitigate this conflict and potential perverse result on security and privacy, we request that the section be updated to clarify that the business maintains the obligation to handle such requests while the service provider's role is strictly limited to informing the consumer to make their request directly with the relevant business with which the consumer interacted.

3. Request for the inclusion of multi-factor authentication as part of identity verification process for privacy rights requests.

Okta is at the forefront of identity verification and promotes using secure practices to enable consumers to delete or access, view, and receive a portable copy of their personal information, in line with reasonable data security controls. According to Trace Security, 81% of company data breaches are due to poor passwords [8] and using multi-factor authentication ("MFA") is an easy way to prevent most cyberattacks and helps protect against fraudulent requests. To avoid having an adverse effect on individual privacy, we believe that the verification process described in section 999.313 (*Responding to Requests to Know and Requests to Delete*) and 999.324 (*Verification for Password Protected Accounts*) of the Proposed Regulations should be robust and include appropriate identity verification steps before permitting access to individuals' personal information.

In section 999.323 (*General Rules Regarding Verification*) of the Proposed Regulations, the AG notes that businesses must account for "the likelihood that fraudulent and malicious actors would seek the personal information" and determine "whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests…". This acknowledgement of potentially fraudulent activity through the verification process prompts the need for the AG to clearly require MFA, when appropriate, as part of the verification process including listing it as one type of "available technology for verification" described in section 999.323(b)(3)(f). The approach to use multiple factors is consistent with privacy guidance recently released to verify identity for responding to individual rights requests under the General Data Protection Regulation, such as to access personal information.[9]

As indicated in section 999.323(d), the verification standards put forward by the AG should prioritize guidance on implementation of reasonable security as part of the process by either (i) requiring businesses that maintain a password-protected account with the consumer to use of MFA to delete or access, view, and receive a portable copy of their personal information under sections 999.313(c)(7) and 999.324 or (ii) making the use of MFA to verify identity based on the existing account details on file as an alternative to collecting additional personal information from an individual for verification in line with the requirements under sections 999.323(c) and 999.325 (*Verification for Non-account holders*). The foregoing clarifications to utilize MFA for verification when appropriate are also consistent with the reasonable security measures to detect fraudulent identity described in section 999.323(d). We encourage lawmakers to look at security frameworks to make sure that privacy processes are developed with security in mind. Requiring the use of MFA is interoperable with existing federal security frameworks [10] and helps to promote more secure identity access management processes for personal information sharing.

In sum, including the requirement to use MFA, when appropriate, would allow the state of California to further aims to both promote privacy and require reasonable security in furtherance of consumer rights.

Conclusion

Okta praises the State of California's work in this area and appreciates the consideration of our views and perspectives. While Okta is firmly in favor of strengthening consumer privacy and security, we also understand the challenges and high compliance costs, productivity losses, and administrative burdens that arise as an effect of disparate regulatory requirements. Okta welcomes further discussions in this area and is happy to serve as a resource for the AG.

Respectfully Submitted,

Okta, Inc.
Privacy and Product Legal Department
[redacted]

[1] "Okta Now Has Over 100 Million Registered Users, Says CEO" - https://finance.yahoo.com/news/okta-now-over-100-million-234824968.html
[2] AB-375 Section 2(h)
[3] https://oag.ca.gov/privacy
[4] AB-375 Section 2(h)
[5] Student Online Personal Information Protection Act, Cal. Civ.Code § 22584(g) does not prohibit operators from sharing aggregated deidentified information for development and improvement.
[6] The General Data Protection Regulation, Recital 50, Further Processing of Personal Data
[7] Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, (l) 11 CCR § 999.314 *Service Providers*, page 22
[8] https://www.tracesecurity.com/blog/articles/81-of-company-data-breaches-due-to-poor-passwords
[9] Rights of data subjects guidance, Autoriteit Persoonsgegeven (Dutch Data Protection Authority) https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#hoe-kan-ik-de-identiteit-vaststellen-wanneer-iemand-zijn-haar-privacyrechten-uitoefent-7212
[10] Draft NIST Special Publication 800-207, Zero Trust Architecture; NIST 800-63, Digital Identity Guidelines; and NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

Message

From:	Barbara Lawler [redacted]
Sent:	12/6/2019 11:08:43 PM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]; Barbara Lawler [redacted]
Subject:	CCPA Proposed Regulations feedback (supplement to 12/4/19 public hearing)
Attachments:	California AG CCPA Public Hearing 12.04.2019 _BLAWLER.pdf

Hello,
Here is the detailed submission from my testimony on Wednesday 12/4/19 in San Francisco. It includes and expands upon my comments that day.

Best regards,
Barb Lawler

--

Barbara Lawler | Chief Privacy and Data Ethics Officer
[redacted]

California State Attorney General CCPA Public Hearings
December 4, 2019
Barbara Lawler, [redacted]

Thank you to **Attorney General Becerra** and staff for holding this forum to provide feedback on the Proposed Regulations. My name is Barb Lawler and I'm the Chief Privacy and Data Ethics Officer of Looker, based in Santa Cruz. I am providing feedback as a 20+ year privacy leader and as a California native. I applaud my home state's ongoing efforts to provide meaningful privacy protections to its citizens.

My feedback today, which will also be submitted in writing with more detail, reflects those 20+ years of building and implementing ethical world-class privacy programs -- as the former CPO of Hewlett Packard, and of Intuit, known for operational excellence and innovative approaches that meet the spirit, policy and legal intent of global data protection regulations, including the CCPA.

With the goal of honoring the new rights enshrined for California consumers, enabling effective compliance by businesses of all sizes and industries, and focused on achieving positive privacy outcomes for consumers, I offer suggestions in three foundational topics:

1) **Clarify the definitions and relationships between a "business", a "service provider" and a "third party"**; these definitions drive all strategic and tactical contracting arrangements and negotiations. The range of interpretations I've seen so far run the gamut from no change in terms, to the same type of companies saying one is a 'service provider' and another is a 'third party', some will sign CCPA addendums and some won't. Definitions overlap beginning with (999.301.d) 'Sources' and (999.301.e) 'Categories of Third Parties', the latter of which many would clearly instead be 'service providers', and yet don't quite align with (999.314.a,.c,.d) requirements for Service Providers. Many Service Providers. We've used a table to map the relationships, but even with a team of expert advisors and peers, I remain concerned that we don't have it right, and that many others don't either.

More specifically, the models used in HIPAA, GLBA and the GDPR are helpful here. It is more straightforward to first structure the relationships based on those between organizations (which will be governed by contracts), and then factor in the relationship to the consumer. Please see the table below, which describes the organizational relationships.

	Organization in control, making decisions, giving directions, determines uses and has primary responsibility for personal information/personal data.	Organization receiving restrictions, requirements and directions and has responsibility to the primary organization, and has no independent use for personal information/personal data, beyond operating their business, providing the product/service.	Organization may receive restrictions or requirements, but has limited or no direct responsibility to the primary organization, and has independent uses for personal information/personal data.
HIPAA	Covered Entity that is a Healthcare provider.	Business Associate to the Covered Entity.	
GLBA	Financial Institution	Third Party provider to the FI.	Affiliates and Partners to the FI
GDPR	Controller	Processor and Sub-Processor	Controller to Controller
CCPA **(as proposed)**	Business	Service Provider Third Party (Definitions are partly interchangeable)	Third Party Service Provider (Several listed as Third Parties are more likely Service Providers)
CCPA ***(recommended)***	Business	Service Provider	Third Party

Examples:

CCPA *(recommended)*	<u>Business</u>: Has the direct relationship with its customers - which could be consumers or other businesses; therefore is the	<u>Service Provider</u>: SaaS, Paas; infrastructure, ISPs, operating systems; B2B online/cloud services such as email service providers, CRM	<u>Third Party</u>: Other Businesses, Partners, Affiliates, Co-branded relationships

	primary data collector).	systems, healthcare ops management, HR management, financial management, cloud hosting and services including analytics	

2) **Streamline the intertwined CCPA notice and privacy policy requirements** (Notices: 999.305.b, .c, 306, 307; and, 308 Privacy Policy) - a fundamental. Did you intend multiple separate notices that link to a privacy policy, or privacy policy that includes the multiple notices embedded? Both? So many notices and so much nested linking - its privacy notice inception! Historically the terms privacy notice and policy are often used interchangeably. So honestly as an 'old timer' who's written all types of privacy policies, statements and notices over many years, these sections gave me a headache, and it feels like a step backwards, although the content is obviously important to convey to consumers.

Start with the Privacy Policy - which should be treated the 'master' or 'global' privacy principles and policy which contains all the information as required in the proposed regulations as well as other legal and policy commitments and organization/business is making. How I wish the CCPA started with and was structured by globally recognized privacy principles (APEC, OECD, FIPPs). That Privacy Policy may either point to a specific subsection within the policy covering the required Notices content, link, list or publish the required Notices content. Simplify the Notices content requirement into one for Notices that contains all the requirements common to each type of Notice, and then call out the unique specifics. A set of model notices would be very helpful here - that could be adapted to an appropriate level of detail based on the type of organization size and industry, its relationship to consumers and personal information collected, shared and sold. Very simply:

- Privacy Policy
  - Notices
    - Notice (999.305)
    - Notice (999.306)

        - Notice (999.307)

More sophisticated companies manage and structure their privacy policy(s) as part of a larger organizational policy structure (both internal and external), which looks something like this:

- Code of Conduct and Ethics
    - Supplier Code of Conduct
    - Acceptable Use Policy (online code of conduct/social media policy)
- Company Values
    - Privacy Policy
        - Privacy Principles
        - Global statutory and legal requirements
            - CCPA
        - Privacy Certs and Seals
            - EU-US Privacy Shield
    - Security Policy
        - Compliance and certifications
    - Human rights commitments or policy
    - Environmental/Sustainability policy
    - EEO/Hiring policy
- Terms of Service/MSLA
    - Data Protection Agreements (GDPR, BAA, CCPA, etc)

One other note: the Regulations state that the Privacy Policy (308.a.2.a) and Notices should be in "plain, straightforward language and avoid technical or legal jargon". The Regulations in their entirety should follow that same principle - regulations don't need to be complex and cumbersome to provide effective guidance. Most reading the Regulations won't be legal, privacy or policy experts, and so the Regulations should be easily understandable by the average person. This will promote compliance.

3) **Consider reducing friction for consumers making legitimate data deletion and right to know requests**. Based on 18 months of GDPR experience, our data says 99% of data rights request are for deletion only, made via the privacy email box. No one really calls , all our support services are provided by 24/7 real-time live chat (we have not had an 800 number or Toll number, or infrastructure built to support one), and no-one really wants to fill out a form. Forms are great for capturing metrics and analytics (something my company Looker excels at). My prediction is for many businesses, the majority will receive emails requesting deletion. The detailed response (999.312.a.-c, and 999.313.a,.c,.d; 999.315.a,.d,.f,.g,.h) and verification requirements may be helpful for some companies, but practically speaking, it seems unlikely that companies will use differing verification standards - and instead set one high standard for response, processing the requests, including verification. The requirements as written favor large established organizations with a lot of resources and pre-existing infrastructure. Consumers will probably perceive the steps and requirements as inhibiting their CCPA rights requests, rather than enabling them. Consumers will perceive the form and verification steps as organizations making it hard for them, which is not the intent of the CCPA or the proposed Regulations. Let's simplify!

Please note my written comments will address additional opportunities:

- The need for positive incentives and accountability frameworks that recognize responsible companies striving daily to be compliant and do the right thing, similar to the EU-US Privacy Shield, Codes of Conduct described in the GDPR, or security Certifications (e.g. ISO27xxx), Privacy Seal programs and similar.
    - I direct you here to the important work being done by the Information Accountability Foundation - on accountable frameworks for big data ethics, including privacy and accountability impact assessment tools that guide organization to assess up front data-driven projects and research, and the possible impacts and outcomes to all stakeholders, including enforcement.
    - http://informationaccountability.org/big-data-ethics-initiative/
    - http://informationaccountability.org/wp-content/uploads/IAF-Big-Data-Ethics-Initiative-Part-B.pdf

- http://informationaccountability.org/wp-content/uploads/Enforcing-Big-Data-Assessment-Processes.pdf

- The need for decision tools, templates (e.g. model notices) and checklists to guide compliance with the statute and regulations - that are easy to read and understand by the average person. Leverage existing excellent resources and best practices from the IAPP, FTC, FPF, the former California Office of Privacy Protection, and others;
  - Note that -- in aiming detailed regulations at large technology companies, smaller companies in other industries that use those same technologies to run their business, with less resources or expertise, may be left confused and uneasy.
- Prioritized guidance for reasonable security expectations -- especially for small and medium businesses. Few are familiar with the CIS20 - much more are familiar with the Safeguards Rule, ISO, NIST, or SOC1/2/3 standards.
- Clarification for cloud-based/B2B services, which seem to have been largely misunderstood or overlooked in the CCPA context.
- The need for an authorized state-provided resource for businesses to confirm the validity of registered authorized agents (999.301.c, 999.326.a, .b) and recommended procedures for validating those who claim Power of Attorney. Without such a service, organizations will apparently be obligated to to take a claim of Authorized Agent or Power of Attorney at face value or by easily manufactured or spoofed proof - a clear opportunity for fraud and scams. Even technical solutions pose a risk as bots or man-in-the middle malware could circumvent controls at scale.
- Clarify the policy and enforcement purposes and intended uses of published 'training metrics' (999.317.a,.b, .e) and the 'calculated value of consumer data' (999.337.b), as these feel like company confidential trade secret, IP or financial reporting information. I appreciate the goal of transparency here, but I have a hard time envisioning any company being comfortable publishing either of these.
  - For training, this is something organizations may provide at externally for specific request under NDA, for an investigatory action or through confidential feedback to Corporate Citizenship NGO reporting.

- For the calculated value of consumer data, except for a few large data centric or data product companies, few if any would be able to do this any time soon. The rest wouldn't know where to start, and would be a financial analysis activity requiring executive sponsorship from the CFO and CEO. Most would consider it very sensitive confidential company information. While there's a lot of talk about "monetizing data" and treating data as an asset, the assumption seems to be that companies have dedicated economists or finance analysts to that activity. Data as an Asset speaks to security and privacy protection, not monetization activity. Monetizing data and the value of a particular data set or project involving dat doesn't start with the kind of ROI calculations envisioned in the proposed Regulations -- the economic value is more likely an outcome or result rather than a balance sheet activity. There's an element of that which goes in annual financial reports to a Board of Directors and the SEC, but probably not the way required under the proposed Regulations.
- Without a clear policy or regulatory objective for each of these that makes sense to an organization's executive team, expect more push-back and resistance to these.

Again, thank you for the opportunity to give feedback on the draft proposed regulations. Please feel free to contact me for a more detailed discussion of my feedback and recommendations. [redacted]

Message

From: Josh Fisher [redacted]
Sent: 12/6/2019 8:31:54 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Regulations Comment Submission
Attachments: Association of Global Automakers - Proposed CCPA Regulations Comments.pdf

Attached are comments from the Association of Global Automakers on the proposed CCPA regulations. Please let us know if there are any questions. Thanks.

Josh Fisher
Senior Manager, State Government Affairs
Association of Global Automakers, Inc. (Global Automakers)
1050 K Street, NW Suite 650
Washington, DC 20001
[redacted]
GlobalAutomakers

GlobalAutomakers

APTIV • Aston Martin • Bosch • BYTON • Denso • Ferrari • Honda
Hyundai • Isuzu • Kia • Local Motors • Maserati • McLaren
Nissan • NXP • Panasonic • PSA • Sirius XM • Subaru • Suzuki
Texas Instruments • Toyota

December 6, 2019

Submitted Electronically at PrivacyRegulations@doj.ca.gov

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Attorney General Becerra:

The Association of Global Automakers, Inc.[1] (Global Automakers) appreciates the opportunity to provide comments on the proposed regulations of the California Consumer Privacy Act (CCPA), which were released by the California Attorney General's Office on October 10, 2019.[2]

We commend the Office of the Attorney General (AG) for its broad solicitation of feedback from diverse stakeholders and the public through public forums and requests for comments regarding the implementation of the proposed regulations. Global Automakers recognizes that privacy is an increasingly important value that all industries must recognize. Motor vehicle manufacturers and the general automotive-related industry aim to provide consumers with greater control over data and transparency with respect to the collection, use, and transfer of data, and to implement technological controls to enhance consumer privacy and ensure accountability with regards to privacy and fair practices.

As the members of the Association of Global Automakers prepare to implement the CCPA, additional clarity regarding various provisions of the proposed regulations would help ensure compliance with the law. Below we discuss specific provisions of the proposed regulations that require the AG's clarification as they are particularly relevant to the members of Global Automakers.

I. Concerns and Requests for Clarification Unique to the Automotive Industry

Global Automakers requests clarification of the following issues that uniquely affect motor vehicle manufacturers and the automotive industry.

a) Enable Automakers to Share Personal Information with Third Party Emergency Response and Roadside Assistance Providers

"Sale" is defined under the CCPA as the "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing or by electronic or other means" the

[1] The Association of Global Automakers represents international motor vehicle manufacturers, original equipment suppliers, and other automotive-related trade associations. Global Automakers works with industry leaders, legislators, regulators, and other stakeholders in the United States to create public policies that improve motor vehicle safety, encourage technological innovation, and protect our planet. Our goal is to foster an open and competitive automotive marketplace that encourages investment, job growth, and development of vehicles that can enhance Americans' quality of life. Our members' share of sales and production in the United States is nearly 45 percent and growing. For more information, visit www.globalautomakers.org.

[2] Proposed CCPA Regulations, Cal. Code Regs. tit. 11, §§ 999.300 – 341 (Oct. 10, 2019).

personal information of a consumer to another business or third party "for monetary or other valuable consideration."[3] Without further clarification, the broad scope of "sale" could be interpreted as prohibiting automakers from sharing a consumer's personal information with emergency service providers absent providing an opt-out.

Many automakers offer emergency response and roadside assistance services to allow consumers to obtain vital, perhaps life-saving, services in the event of an emergency. Some emergency or roadside assistance services may be provided by third party for-profit entities that, in addition to providing these vital services, also retain and use personal information for their own purposes such as maintaining relationships with consumers for additional services.

Sharing personal information with such entities may be considered a sale under the CCPA to the extent they are not acting solely as a service provider. If a consumer requests that an automaker no longer sell the consumer's personal information, the CCPA could be interpreted as prohibiting the automaker from sharing the consumer's personal information with emergency service providers absent express re-authorization. Requiring a consumer to provide such authorization may delay or prevent the delivery of emergency services.

To facilitate the delivery of emergency response or roadside assistance services subject to a consumer request or automated crash notifications, Global Automakers requests that the Attorney General adopt regulations authorizing the sharing of personal information with third party providers of such services, even if the consumer associated with the vehicle has previously requested the automaker to not sell their personal information.

b) Clarify the "Notice at Collection" Requirements for Automakers

According to the proposed regulations, businesses must inform consumers of the categories of personal information to be collected and the purposes for which the personal information will be used "[a]t or before the point of personal information collection."[4] Businesses that do not collect information directly from consumers do not need to provide notice at collection to the consumer, but in order to sell a consumer's personal information must either: (i) contact the consumer directly to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out, or (ii) contact the source of the personal information to confirm that the source provided a notice at collection to the consumer and "obtain signed attestations from the source describing how the source gave notice at collection" with an example of the notice included.[5]

While we support the proposed guidance on how to provide notice to consumers at collection, we request the AG provide additional clarification of the downstream application of these regulations. Global Automakers' concern regarding providing notice at the time of collection of personal information arises from the unique nature of automakers and other businesses that collect personal information from

[3] Cal. Civ. Code §1798.140(t)(1) (proposed).

[4] Cal. Code Regs. tit. 11 § 999.305(a)(1) (proposed).

[5] Cal. Code Regs. tit. 11 § 999.305(d)(2) (proposed).

connected devices that may have a future change in owner. Automakers will face significant challenges in providing such notice to vehicle owners and drivers beyond the initial purchaser of the vehicle.

When a vehicle is transferred from one owner to another, automakers do not receive notice of the transfer for days or months, if ever. During this time the transferred vehicle may continue to transmit vehicle health and crash-related information to the automaker, based on permissions granted by the original owner. Information collected from the vehicle post-transfer may constitute personal information of the new owner as the information may be associated with a Vehicle Identification Number ("VIN"), which may be linked to the new owner, in a DMV database, even if the automaker does not have that information. Providing notice to vehicle owners and drivers beyond the initial owner of the vehicle is challenging as many connected vehicles, particularly used vehicles, are not equipped with displays that can be configured to provide notice as required by the proposed regulations at time of collection. Even if they are, the time lag in notice of an ownership change fails to provide automobile manufacturers with notice of when to trigger refreshed, in-vehicle notice. Owners' manuals are not always transferred to subsequent owners.

Global Automakers urges the Attorney General to clarify that automakers and other businesses that collect personal information from connected devices that may have a change of owners without notice that § 999.305 can be complied with by providing publicly available, online privacy policies that contain the required disclosures.

The proposed regulations also state that businesses may obtain signed attestations from the source of the personal information to confirm that notice was provided at the time of collection. Global Automakers supports this proposed regulation generally as it reasonably addresses the challenges that businesses face when collecting personal information from sources other than directly from the consumer, while establishing controls designed to confirm that consumers have received upstream notice of sales of personal information and the opportunity to opt-out.

However, the proposed regulation does not expressly state that businesses need only obtain a single attestation from each source describing how notices are provided to consumers, or the frequency over which these attestations need be renewed. Sources of personal information and businesses may be required to consistently refresh attestations, which would incur storage and transmission costs along with administrative burden in keeping track of attestations received and requested. So long as businesses receive from sources examples of the notices that consumers actually received, a single attestation would reasonably address the proposed regulation's requirements. We further request that the Attorney General clarify how often the attestations from sources must be obtained. In many instances, contracting parties share a continuous "flow" of personal information after the contract is executed. Clarifying that the attestations can be obtained on a one-time basis, annually, or with every set of consumer personal information received by the business would provide guidance to businesses on how to comply with the CCPA in their contracts.

c) The Requirement to Notify Third Parties of Opt-Out Requests Should Reflect Consumer Preferences

The CCPA requires businesses to implement opt-out requests from consumers by ceasing the sale of personal information after receiving the request, but does not require businesses to pass these opt-out notices along to previous recipients of the requestor's personal information. Put another way, the CCPA does not make opt-outs apply retroactively.[6] However, proposed regulation § 999.315(f) requires businesses receiving opt-out requests to identify the third parties to which they sold personal information in the 90 days preceding the requests and instruct them to not further sell the information.

Our concern regarding the notification of third parties is twofold. First, the proposed regulations are unclear as to whether the third party is also obligated to continue to pass the opt-out request down the chain to others to whom they may have sold data. If interpreted this way, the proposed regulation would restrict the flow of data that many businesses rely upon to provide services to consumers and creates significant challenges for businesses when clawing back data that has been passed on to third parties.

A second concern is that requests to third parties may conflict with consumer preferences. While a consumer may wish to prohibit a specific business from selling the consumer's personal information going forward, a consumer may not intend for their opt-out request to apply to anyone except the business. In one example from the automotive industry, a vehicle owner may appreciate, and even benefit from, receiving advertising and other communications provided by third parties that are personalized based on personal information collected from prior commutes. When the consumer exercises the right to opt-out of the sale of personal information from an entity it knows, the consumer may not intend to opt-out of services provided by different businesses.

These concerns are exacerbated by the fact that entities affiliated by name, but not corporate ownership, are not allowed to share personal information freely. This challenge is acute in the context of the information exchange between automakers and independent auto dealerships that share common branding. It is common for automakers and their independent dealers to share vehicle-related information to support repair services, discount programs, and other jointly-managed operations that benefit consumers. The proposed regulations require the automaker to pass along a consumer opt-out to their dealers, if the consumer's personal information was disclosed to the dealer in the previous 90 days.[7] Consumers may not understand that automakers and their independent dealers are not affiliated by common ownership. As a result of requiring opt outs to be passed to third parties, consumers may unknowingly globally opt-out of the sharing of their information between automobile manufacturers and independent dealers that enables them to receive the services they currently utilize. Global Automakers requests that the AG clarify that businesses do not need to pass opt-out requests to third parties to avoid the aforementioned consequences.

d) Clarify that Personal Information Associated with Multi-User Devices Should be Treated in a Manner Similar to the Proposed Approach for Household Information

Proposed regulation § 999.318 provides that if a consumer does not have a password-protected account with a business, requests to access personal information may be addressed by providing aggregate

[6] Cal. Civ. Code § 1798.120(d).

[7] Cal. Code Regs. tit. 11 § 999.315(f) (proposed).

information. This proposal addresses concerns that unauthorized persons may obtain information about other household members via access requests. The mere fact that a person is associated with a household should not result in businesses having to disclose to that person all personal information associated with household members.

Similar concerns arise in the context of multi-user devices (e.g., shared vehicles). When a user of a multi-user device requests access to personal information, businesses should be permitted to provide aggregate information to avoid disclosing personal information to unauthorized individuals. Disclosures of specific pieces of personal information associated with the multi-user devices should be required only where all users jointly request such access and the business is able to individually verify all requests. Similarly, businesses should not be required to delete household or multi-user device information unless all household members or device users have issued verified requests to do so. Global Automakers requests that the AG clarify that personal information associated with multi-user devices be treated in the same manner as household information with regards to access and deletion requests.

Global Automakers also request that the AG clarify "household" in the definition of "personal information." The proposed regulation broadly defines "household" as "a person or group of people occupying a single dwelling."[8] It is unclear what is considered a "single dwelling" and whether transitory dwellings such as dormitories or rooming houses can be considered a single dwelling with multiple occupants. The AG should clarify the definition of a "household" to provide further guidance for businesses.

e) Clarify that Vehicle Information Collected to Identify Safety and Quality Issues Is Not Subject to Requests to Delete

The CCPA permits a business that receives a verifiable request from a consumer to delete personal information to refuse the request if the business maintains the personal information to enable "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."[9] It is unclear if vehicle information that may be maintained by motor vehicle manufacturers for internal safety and quality analysis falls under this exemption.

It is also unclear if vehicle information collected for these safety and quality purposes falls under the exemptions provided for in Assembly Bill 1146 ("AB-1146"). In recognition of the need for additional exceptions for businesses who keep consumer information for warranty and safety purposes, the California legislature passed AB-1146 on October 11, 2019, which provides that vehicle information or ownership information retained or shared between a new motor vehicle dealer and the vehicle's manufacturer is exempt from the CCPA's right to opt-out if the information is related to repairs made under warranty or to conduct recalls. However, motor vehicle manufacturers routinely retain vehicle information for safety and quality analysis purposes that may not lead to a recall. It is unclear if such information falls into the exemption provided under AB-1146.

Information collected from the vehicle may constitute personal information of the vehicle owner as the information may be associated with a Vehicle Identification Number ("VIN"). This information gives motor vehicle manufacturers the ability to conduct safety and quality analysis that consumers would

[8] Cal. Code Regs. tit. 11 § 999.301(h) (proposed).

[9] Cal. Civil Code § 1798.105(d)(7).

expect of vehicle manufacturers. The proposed regulations do not clarify if this information is exempt from the right to delete or right to opt-out under the CCPA. Global Automakers requests that the AG clarify and provide guidance with respect to the required obligations regarding vehicle information.

f) Clarify that Proprietary Information Relating to Trade Secrets and Intellectual Property Rights is Not Subject to Requests to Know

The proposed regulations reference that a business may deny a consumer's verified request to know specific piece of personal information because of conflict with federal or state law but does not clarify the CCPA's exceptions relating to trade secrets and intellectual property rights, which may arise from common law.[10] Moreover, the CCPA provides that the AG will establish any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights. In certain cases, companies may need to disclose personal information to the consumer that references such proprietary information. Global Automakers requests that the AG provide guidance with respect to the applicability of the exception to respond to trade secret or intellectual property rights.

II. Provisions that Would Benefit from AG Clarity

In addition to the items discussed above, Global Automakers would like to highlight several aspects of the proposed regulations that would benefit from additional clarity. These issues are not unique to the automotive industry. Nevertheless, we believe the experiences of our members are helpful in understanding the potential real-world impact of implementing the proposed regulations as written.

a) Clarify that Precise Geolocation Data is Not Subject to Requests to Know

The proposed regulations state that a "request to know" is "a consumer request that a business disclose personal information that it has about the consumer…."[11] In response to "requests to know," a business must not "disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers."[12] Global Automakers commends the Attorney General for clarifying the categories of information a business may not disclose as disclosure of these specific pieces of information to unauthorized individuals creates significant privacy risks for consumers.

To further protect consumers, we request that the AG clarify that precise geolocation may be disclosed by companies pursuant to a "request to know" only if there is a reasonable basis to do so. The Federal Trade Commission has recognized that precise geolocation is sensitive information in that it has the potential to reveal family, political, religious, and sexual associations.[13] Precise geolocation data may also be used by abusers to track and harm estranged spouses, domestic partners, or others. For these compelling public policy reasons, Global Automakers requests that the AG clarify that companies may perform a risk assessment to determine if disclosure of geolocation data may pose a risk to the safety or security of a consumer before transmitting this personal information.

[10] Cal. Code. Regs. tit. 11 § 999.313(c)(5).

[11] Cal. Code Regs. tit. 11 § 999.301(n) (proposed).

[12] Cal. Code Regs. tit. 11 § 999.313(c)(4) (proposed).

[13] *See* FTC, Protecting Consumer Privacy in an Era of Rapid Change 34 n.8 (2012), *available at* https://bit.ly/1SHOpRB.

b) Clarify that Businesses May Comply with Category-Disclosure Requirements by Providing General Business Practices and Categories

Under proposed regulation § 999.313(c)(9), a business is required to provide an individualized response to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties. The regulation provides that the individualized response "shall not refer the consumer to the businesses' 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."[14] Proposed regulation § 999.313(c)(10) further provides that a business shall provide for each identified category of personal information it has collected about the consumer: (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.[15]

Requiring businesses to provide an "individualized response" to each consumer about categories of personal information, categories of sources, and categories of third parties creates significant compliance challenges. In order to provide such individualized responses, businesses would need to build the technical infrastructure required to associate personal information by source, customer, and use(s) in order to enable the business to provide responses specific to individual customers. This would prove nearly impossible to comply with, as many businesses that do not currently track information in this manner. Such efforts may also prove to be unsuccessful considering the challenges of aligning generalized categories to what is happening with a specific consumer.

c) Clarify Scope of User-Enabled Privacy Controls for Opt-Out Requests

Proposed regulation § 999.315(c) would require user-enabled privacy controls to be treated as opt-out requests by businesses that collect personal information from consumers online. The regulation states that browser plugins and privacy settings may serve as such controls, but the regulation does not provide a definition of what constitutes "user-enabled privacy controls." A wide range of user-enabled privacy controls exist including those developed through industry efforts to those created by consumers, such as customized browser add-ons that can send a signal that the consumer interprets as an opt-out. Given the broad range of potential signals and online collection channels including traditional websites, vehicles, wearables, and other connected devices, businesses may not be able to determine whether a signal transmitted online constitutes a "user-enabled privacy control."

To provide clarity to businesses and to provide assurances to consumers that businesses will understand opt-out signals, Global Automakers requests that the AG clarify that "user-enabled privacy controls" will constitute opt-out requests only if businesses affirmatively claim to respond to the controls or if the AG endorses such controls through regulation for specific online collection channels.

[14] Cal. Code Regs. tit. 11 § 999.313(9) (proposed).
[15] *Id.*

d) Clarify the "Reasonable Security Measures" Required in Transmitting Personal Information to the Consumer

The CCPA permits a business that receives a verifiable request from a consumer to access personal information to deliver that information to the consumer by mail.[16] The proposed regulations further state that businesses must "use reasonable security measures when transmitting personal information to the consumer."[17] In certain cases companies may need to transmit personal information to the consumer by mail, particularly with individuals who do not have electronic accounts with the business. The proposed regulations are unclear as to reasonable security measures must be taken within the context of using U.S. mail. Global Automakers requests that the AG clarify and provide guidance with respect to the required security measures.

III. Summary

Global Automakers and our members appreciate the opportunity to comment on the proposed regulations of the California Consumer Privacy Act and look forward to continuing to work with the CA AG on these issues.

Please feel free to contact me should you have any questions.

Sincerely,

Josh Fisher

Josh Fisher
Senior Manager, State Government Affairs
[redacted]

[16] Cal. Civ. Code §1798.100(d).

[17] Cal. Code Regs. tit. 11 § 999.313(c)(6) (proposed).

Message

From:	Katey M. Herman [redacted]
Sent:	12/6/2019 11:39:19 PM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC:	Jenny J. Rim [redacted]
Subject:	CCPA Regulations Comments
Attachments:	CCPA Backups Comment (2019-12-06).pdf

Dear Privacy Regulations Coordinator,

Attached is a written comment in response to the proposed CCPA regulations, signed by Pharmavite, LLC, Piping Rock Health Products, LLC, Astex Pharmaceuticals, Inc., and Avanir Pharmaceuticals, Inc. Thank you.

Regards,

Katey Herman

Katey Herman
Senior Counsel, Legal Affairs

Pharmavite LLC
8531 Fallbrook Ave.
West Hills, CA 91304
[redacted]

This email message is for the sole use of the intended recipient(s). If you are not the intended recipient, please contact the sender by reply email, delete the original message and any copy of it from your computer system, and destroy all printed copies. This email may contain confidential and legally privileged information; to the extent it does such information must be treated as confidential. Any unauthorized review, use, disclosure or distribution is prohibited.

astex pharmaceuticals PHARMAVITE AVANIR pharmaceuticals PipingRock

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Proposed California Consumer Privacy Act Regulations

Comments of Pharmavite, LLC; Astex Pharmaceuticals, Inc.; Avanir Pharmaceuticals, Inc.; and Piping Rock Health Products, LLC

Our companies understand and respect the importance of consumer privacy, and we support the efforts of the California Legislature and Attorney General to codify meaningful protections for California residents. We respectfully submit the following comments on the Attorney General's draft regulations.

Background About Our Companies

Pharmavite, LLC ("Pharmavite") manufactures and markets Nature Made® dietary supplements. For more than 45 years, Pharmavite has made and distributed high quality vitamins, minerals, herbs, and other dietary supplements that promote wellness and help maintain good health. Pharmavite, a subsidiary of Otsuka America, Inc., is headquartered in West Hills, CA and has manufacturing and distribution facilities in San Fernando and Valencia, CA, and in Opelika, AL.

Piping Rock Health Products, LLC is a vertically integrated company that manufactures and markets supplements and essential oils. Backed by a team of experts with over 40 years of experience in the industry, Piping Rock is committed to developing and delivering only the highest quality vitamins, herbal supplements, ingredient-based topical products and pure plant based essential oils. Piping Rock Health Products is headquartered in Ronkonkoma, NY and has manufacturing and distribution facilities across New York, Ohio, and California.

Astex Pharmaceuticals, Inc. ("Astex") was formed through the merger of Astex Therapeutics Limited (UK) and SuperGen, Inc. (US) in 2011. The company was subsequently acquired by Otsuka (Japan) in October 2013. Astex continues to build a rich product portfolio with multiple drugs in clinical development. Our corporate mission is to discover and develop novel therapeutics with a primary focus in cancer.

Avanir Pharmaceuticals, Inc. is a biopharmaceutical company focused on bringing innovative medicines to patients with central nervous system disorders of high unmet medical need. As part of our commitment, we have extensively invested in our pipeline and are dedicated to advancing medicines that can substantially improve the lives of patients and their loved ones. Avanir is headquartered in Aliso Viejo, CA and is a subsidiary of Otsuka America, Inc.

The Regulations Should Permit and Encourage Businesses to Frequently Backup Data and Test Disaster Recovery Plans.

We are pleased that the Attorney General's draft regulations acknowledge that deletion requests for personal information stored in backup or archival systems raise difficult, unique technical challenges. Section 999.313(d)(3) of the draft regulations rightly acknowledges that businesses may have limited ability to implement a request for deletion immediately with respect to backups. However, the proposed requirement for a business to delete personal information stored in a backup when it is "is next accessed or used" is ambiguous, and potentially inconsistent with the state of the art of backup management and disaster recovery.

To more squarely address the technical challenges with accessing specific data stored in backup or archival systems, encourage businesses to develop and test disaster recovery plans, and protect consumers' interest in having their rights requests honored and data protected, the Attorney General should revise the draft regulations to clarify that routine and necessary activities related to maintaining viable data backups, such as integrity checking and incident response drills, do not trigger the requirement to comply with a deletion request pertaining to backed up or archived personal information. While deletion requests should be executed prior to any backed up data being restored and used in a production environment, a rule that requires compliance (*e.g.*, deletion) prior to that point would discourage businesses from backing up or testing their backups regularly and ultimately harm consumers.

Data Recovery Testing Should Not Trigger Deletion Obligations

A business should not be able to effectively circumvent a consumer's prior deletion request by restoring their personal information from a backup file into a production system. However, "access[] and use[]" could each be construed to include other, routine interactions with backups. Large-scale enterprise backup systems are designed to store and rapidly recover business applications and data and may not provide for the selective deletion of specific data (*i.e.*, at an individual consumer level) within the backup set. In fact, many backup systems store backups in snapshot files or data bundles and do not have the capability to surgically remove a specific record or information from the backup set itself. To reduce the amount of storage used, commercial backup systems often analyze past backups to identify duplicative information, creating incremental backups that include only information changed since the previous backup. These processes, along with any disaster recovery testing, could be construed as "access" or "use," which could effectively destroy the exception—businesses often make incremental backups on at least a daily or even hourly basis.

When personal information is stored in an inactive system, such as a backup or archival system, it poses lower risks to consumers—businesses generally do not analyze data in backup systems, use such data for marketing, or sell it. Moreover, a regulation that requires businesses to delete personal information from archived data anytime it is "accessed" for backup administration purposes only would unfairly harm California consumers while seeming to provide little benefit. As discussed above, enterprise-grade backup software routinely accesses backed up files for a variety of purposes, all of which are meant to ensure that a backup works when needed.

Consumers Expect Businesses to Maintain Robust Backup and Failover Procedures

Consumers expect that businesses will maintain their data securely and continue providing services even if their data centers are hit by natural disaster or other threats. Consumers are harmed when such businesses cannot access necessary data, and a policy that makes backup and recovery processes more difficult, cumbersome, or time-consuming may result in more businesses with recovery plans that do not work fully when disaster strikes. Consumers rely on businesses to maintain the integrity of their data for a variety of purposes from reordering products to recalls and other safety notifications. Should a business be unable to recover its data after an incident, or should there be a delay, consumers relying on these alerts and notifications could be harmed. Therefore, the Attorney General should implement regulations that encourage businesses to develop robust backup systems.

A Variety of Legislatures, Regulators, and Law Enforcement Agencies Encourage or Mandate Regular Backups and Recovery Testing

The Attorney General should *encourage* businesses to engage in best practices with respect to personal information entrusted to them by consumers, including data backups. Many businesses are required by law or regulation to not only maintain backups, but to test backups on a regular basis. These tests help verify that a business can recover from a catastrophic event, whether fire, power outage, earthquake, or a cyberattack. When testing backups, we test our ability to access the data and restore it. We do not, nor do we have the ability to, modify the backups that we test. Yet, under the proposed rule, such tests could trigger an obligation to implement deletion requests within the backup files.

In addition, governmental authorities and cybersecurity experts increasingly advocate that businesses not only backup their data regularly, but test those backups to insure business continuity. One example that is increasingly impacting California businesses is ransomware, which costs businesses, consumers, and the state significant and increasing amounts of time and money each year. For example, the U.S. Department of Justice writes that "[o]rganizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures" to mitigate the risk of ransomware.[1] Under the draft regulations, following the Department of Justice's advice and testing a business's ability to revert from backups could impose significant additional burdens on a business—requiring that it modify the backups to remove information consumers have requested to be deleted, even though the test will not result in their data being used by the business for any commercial purpose, and even though the purpose of the test is to verify the integrity of the original backup—not a modified one.

[1] U.S. Dept. of Justice, *RANSOMWARE: What It Is and What To Do About It*, https://www.justice.gov/criminal-ccips/file/872766/download

Recommended Changes

To confirm that consumers who wish to have their personal information deleted can be sure their personal information will not be actively used by a business after they request deletion, and to encourage businesses to engage in good data practices such as regular backups with robust, state-of-the-art software, we suggest that the Attorney General revise the draft regulation as follows:

Section 999.313(d)(3) If a business stores any personal information on archived or backup systems, it may comply with the consumer's request to delete, with respect to data stored on the archived or backup system **by implementing reasonable safeguards and practices to ensure that Personal Information subject to a deletion request is not restored to an active system from the archived or backup system or otherwise used for any commercial purpose.**

Sincerely,

/s/ D. Jeffery Grimes

D. Jeffery Grimes
Vice President, Corporate
Counsel & Compliance Officer
Astex Pharmaceuticals, Inc.

/s/ Jason Olin

Jason Olin
Senior Director, Assistant
General Counsel
Avanir Pharmaceuticals, Inc.

/s/ Paul Bolar

Paul Bolar
Vice President,
Regulatory Affairs
Pharmavite, LLC

/s/ Irene Fisher

Irene Fisher
General Counsel
Piping Rock Health
Products, LLC

December 6, 2019

Message

From:	Rustici [redacted]
Sent:	12/6/2019 5:40:13 PM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject:	CCPA Regulations
Attachments:	CCPA Comments.docx

For the kind attention of the
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Please find my comments in the attached word document

Kindest regards,
Chiara Rustici

Sent with [redacted]

CCPA Regulations: Comments by Chiara Rustici

Combined effect of CCPA 1789.115 and CCPA 1798.140 (t)(2)(D) 11; expanding CCR § 999.337 (b): Calculating the Value of Consumer Data

Chiara Rustici is an independent academic researcher and data regulation analyst based in the European Union. Having researched the impact of the EU General Data Protection Regulation on data business models for several verticals and on businesses of different sizes and stages of maturity, she respectfully submits to the Attorney General an informed, pragmatic, business perspective on phrasing within CCPA that may create perverse market incentives capable of defeating the policy goals of the regulation itself

CCPA Regulations: Comments by Chiara Rustici

Combined effect of CCPA 1789.115 and CCPA 1798.140 (t)(2)(D) 11; expanding CCR § 999.337 (b): Calculating the Value of Consumer Data

Legal loophole? Perverse market incentives

The text of the CCPA, Section 9, 1798.140 (t)(2)(D) reads:

"For purposes of this title, a business ***does not sell*** personal information when:

[...]

The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120.

[Type sidebar title]

[Type the sidebar content. A sidebar is a standalone supplement to the main document. It is often aligned on the left or right of the page, or located at the top or bottom. Use the Drawing Tools tab to change the formatting of the sidebar text.]

This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code)."

When the subparagraph quoted above is read in conjunction with Section 4, 1798.115 (d), quoted below, it would *prima facie* appear that the obligation by a business to inform consumers that their information is being sold and inform them that they have a 1789.120 right to opt out of that sale is triggered exclusively for **those 3rd parties to whom personal information has been sold**.

By not amounting to a sale, a merger or acquisition or transfer after bankruptcy, therefore, appears to relieve the acquiring business of that obligation: *prima facie* the resale, by the third party, of the consumers' personal information is conditional **not upon** giving the consumer notice of sale and opportunity to exercise their right to opt out of the sale (because obtaining personal information through M&A does not count as having acquired it via a sale of personal information) but merely upon:

- using or sharing personal in a manner that is **not materially inconsistent** with the promises made at the time of collection information, and

- using it or sharing it consistently with 1798.110 and 1798.115.

In fact, CCPA, Section 4, 1798.115 (d), reads:

"Sec. 4. Section 1798.115 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

[...]

(d) A third party shall not sell personal information about a consumer that has been ***sold*** to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120. "

The perverse market incentives created by a literal reading of the CCPA text

It is politely submitted that perverse market incentives might be prevented by expanding CCR § 999.337 (b): Calculating the Value of Consumer Data to account for market practices.

A well-known revenue business model for the start-up ecosystem is to acquire, as fast as possible, as many "users" as possible.

Once scale has been thus secured, the start-up becomes an attractive acquisition target for established businesses precisely because it will allow the buyer to secure ownership and control of the "users' personal information" collected by the acquisition target.

"Users" need not be paying customers: no money needs to change hands to become a "user".

Start-ups need not demonstrate profitability to become attractive acquisition targets, only evidence of "an active user base".

The value of consumers' information created through the sale of the start-up to the established business is left unaccounted for by Section 9, 1798.140 (t)(2)(D) of the CCPA in those cases where:

- the start-up circumvents any CCPA obligations to report the value of consumers' information **before the sale** because it falls outside of the CCPA definition of a covered business in that:

> its annual gross revenues **<u>are not</u>** in excess of twenty-five million dollars ($25,000,000);
>
> or the start-up annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of **<u>less than</u>** 50,000 consumers, households, or devices;
>
> or the start-up derives **<u>less than</u>** 50 percent of its annual revenues from selling consumers' personal information;
>
> or the start-up is treating its users not as paying consumers but as "members", as is the case for .org not-for-profits; or "readers", as is the case of forums which require accounts in order to post comments; or "unique visitors to its website" as is the case of online content sites that use tracking technology to uniquely identify their monthly active readers or, alternatively

- the established business and prospective buyer of start-ups circumvents any CCPA obligations to report the value of consumers' information **after its acquisitions** by acquiring exclusively not-for-profit start-ups, i.e., those that do not pursue revenue growth but only scale of users and thus fall outside the definition of a CCPA covered business.

In this latter case, neither acquisition target, not acquirer may ever become "covered businesses" for CCPA purposes.

Conclusion

The perverse market incentives created by a literal interpretation of the CCPA for both start-ups can thus be summarized:

1) Collect personal information, and sell the business upon securing your 49,999th customer;
2) Collect personal information, and sell the business before reaching annual revenue of $25,000,000
3) Collect personal information as a .org, not-for-profit association, and sell the business as such
4) Maintain your annual revenues from selling personal information below 50% of your total annual revenues until the sale of your business

The perverse market incentive created by a literal interpretation of the CCPA for established businesses on the lookout for acquisition targets can thus be summarized:

5) Only acquire businesses that are ostensibly not-for-profit to secure large amounts of personal information the sale of which consumers cannot opt out of

If my reading of the CCPA text is correct, M&As and transfers post bankruptcies would amount to a form of "laundering" of consumers personal information, lifting any CCPA 1798.120 obligation from the acquiring business.

I have reason to believe this is not the intended policy goal of the CCPA and that a tighter drafting of the Regulations might assist in preventing this literal reading.

With kindest regards,
Chiara Rustici

Message

From:	Wayne Sisk [redacted]
Sent:	12/6/2019 6:44:57 PM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC:	Compliance [redacted]
Subject:	CCPA rulemking activities - Commentary on the proposed regulations
Attachments:	CCPA Hearing notes 12-6-2019 .docx

From:

Wayne Sisk
Sr. Manager of Security and Compliance and Data Protection Officer
Celigo Inc.
[redacted]

See attached if a separate document is desired

Where is the Button? We NEED the [Do Not sell my Info" graphics!] Another round of public comment puts us WAY PAST Jan 1!

- We are drafting our responses based on the codes as written, and now the DRAFT Regulations:

- When will this be final? And will we be given time after that to comply? - How much time?

Main Topic;

These regulations as drafted, do not directly define what constitutes **A Consumer**, or what constitutes **"personal" information**:

"Typical consumer" means a natural person residing in the **United States**. - S/B California and California Residents

The reason I believe defining what constitutes "personal information" is the CCPA reg only partially define this, and there are other older California privacy PII definitions that are more expansive. In addition, **I want to primarily focus on separation of Personal Information and the information about a Corporate Persona:**

No question that John Doe@Gmail.com., or Yahoo.com, or Hotmail and the like, or any other Public Email systems, **as well as my Personal Phone number**, is definitely part of anyone's personal profile and is PII.

- Email is an endemic part of doing business today worldwide.
- **Is "John Doe, @Corp dot com, a person and my personal info?**

    - NO! It is a Corporate Persona...

- A business phone number is also part of my Corporate Persona. - is that "PII? - NO!
- The address of my business? No....

These should be defined, **and excluded**, from this whole notion of PII. it's a **disposable Corporate Persona** and IT's NOT ME. **- Point in fact: I've had dozens of these Corporate Personas. None of them are "ME"; -** It is a **Corporate Persona**, and how I communicate with others, strictly in a business activity, both internally and externally to the company.

A good example of this exclusion is in some of Canada's privacy legislation - they provide an exception for these Corporate Personas!

For Email it's easy - if it's a Corp Email then its excluded. **John Doe @SomeCorporation.com is not me!** The same name, @Gmail.com, would be me... Public Email services...

Phone Numbers-
The endemic use of personal Cell Phones used for business is tricky, but not excessively so - **It is a minimal cost to have a second phone number on the same device.** if someone decides to NOT avail themselves of this, **they have abandoned the concept of their phone number being "private".**

Moreover, I don't see the issue, since many private phone numbers are still being listed publicly, both in paper phone books and online... This legislation does NOT address this at all...

Even having an "unlisted number" is moot as the landline companies have always CHARGED to have an unlisted phone number...

Company address? Moot - for most it is absolutely public information.

Impacting Business to Business information is a pointless hassle imposed for no real gains in privacy at all! In fact, it dilutes the effort to real personal privacy.

Individual Privacy should be the concern here. Not an essentially faceless **Corporate Persona**.

New Topic:
Deleting Information about Employees

- What about Employees of a business? That information is certainly needed and necessary and cannot be reasonably deleted. Updated? Fine, deleted - No, All records of employment must be kept as mandated by other laws... This use of personal needs to be explicitly exempted from the regulation. Especially since most of the time, this data MUST be retained for 30 years or more post retirement… (permanently in the case of anything to do with Haz mat materials exposure for instance.)

Another new Topic - More important: Actual Information Abuses are NOT being addressed:

Companies are now harvesting information from anyone that contacts them, for any reason!

My email gets Spam:

- Shortly after I contact them as a customer of theirs
- Or, in the case of my Business Email**, and I contact a customer**, they immediately spam my business Email. Collection of this information is endemic and getting worse!

I'm also getting Spam Email from companies, both as a Corp Persona and as a personal PII persona, merely for visiting the website

- **I NEVER accept cookies,** so they are collecting my IP address anyway, and cross referencing my IP which has been mapped to my email Via Big Data - and Voila! Instant Email spam!

No individual can hope to chase these "Big Data" misuses with any success, and the data is being propagated and sold without any permissions asked or received.

This legislation and regulation, if it is really going to be effective, should be addressing those misuses directly; **An "Opt Out" button, no matter how available, is like holding up a hand to stop a tidal wave.** You, as an individual are going to be washed away...

Cheers!

Wayne

Wayne Sisk CISA, CRISC | Sr. Manager, Security and Compliance, Data Protection Officer

celigo

O

[redacted]

From:

Wayne Sisk
Sr. Manager of Security and Compliance and Data Protection Officer
Celigo Inc.
[redacted]

Where is the Button? We NEED the [Do Not sell my Info" graphics!]
Another round of public comment puts us WAY PAST Jan 1!

- We are drafting our responses based on the codes as written, and now the DRAFT Regulations:

- When will this be final? And will we be given time after that to comply? - How much time?

Main Topic;

These regulations as drafted, do not directly define what constitutes **A Consumer**, or what constitutes **"personal" information**:

"Typical consumer" means a natural person residing in the **United States**. - S/B California and California Residents

The reason I believe defining what constitutes "personal information" is the CCPA reg only partially define this, and there are other older California privacy PII definitions that are more expansive. In addition, **I want to primarily focus on separation of Personal Information and the information about a Corporate Persona:**

No question that John Doe@Gmail.com., or Yahoo.com, or Hotmail and the like, or any other Public Email systems, **as well as my Personal Phone number**, is definitely part of anyone's personal profile and is PII.

- Email is an endemic part of doing business today worldwide.
- **Is "John Doe, @Corp dot com, a person and my personal info?**
    - NO! It is a Corporate Persona...

- A business phone number is also part of my Corporate Persona. - is that "PII? - NO!
- The address of my business? No....

These should be defined, **and excluded**, from this whole notion of PII. it's a **disposable Corporate Persona** and IT's NOT ME. **- Point in fact: I've had dozens of these Corporate Personas. None of them are "ME"; -** It is a **Corporate Persona**, and how I communicate with others, strictly in a business activity, both internally and externally to the company.

A good example of this exclusion is in some of Canada's privacy legislation - they provide an exception for these Corporate Personas!

For Email it's easy - if it's a Corp Email then its excluded. **John Doe @SomeCorporation.com is not me!** The same name, @Gmail.com, would be me... Public Email services...

Phone Numbers-
The endemic use of personal Cell Phones used for business is tricky, but not excessively so - **It is a minimal cost to have a second phone number on the same device.** if someone decides to NOT avail themselves of this, **they have abandoned the concept of their phone number being "private".**

Moreover, I don't see the issue, since many private phone numbers are still being listed publicly, both in paper phone books and online... This legislation does NOT address this at all...

Even having an "unlisted number" is moot as the landline companies have always CHARGED to have an unlisted phone number...

Company address? Moot - for most it is absolutely public information.

Impacting Business to Business information is a pointless hassle imposed for no real gains in privacy at all! In fact, it dilutes the effort to real personal privacy.

Individual Privacy should be the concern here. Not an essentially faceless **Corporate Persona**.

New Topic:
Deleting Information about Employees

- What about Employees of a business? That information is certainly needed and necessary and cannot be reasonably deleted. Updated? Fine, deleted - No, All records of employment must be kept as mandated by other laws... This use of personal needs to be explicitly exempted from the regulation. Especially since most of the time, this data MUST be retained for 30 years or more post retirement… (permanently in the case of anything to do with Haz mat materials exposure for instance.)

Another new Topic - More important: Actual Information Abuses are NOT being addressed:

Companies are now harvesting information from anyone that contacts them, for any reason!

My email gets Spam:

- Shortly after I contact them as a customer of theirs
- Or, in the case of my Business Email**, and I contact a customer**, they immediately spam my business Email. Collection of this information is endemic and getting worse!

I'm also getting Spam Email from companies, both as a Corp Persona and as a personal PII persona, merely for visiting the website

- **I NEVER accept cookies,** so they are collecting my IP address anyway, and cross referencing my IP which has been mapped to my email Via Big Data - and Voila! Instant Email spam!

No individual can hope to chase these "Big Data" misuses with any success, and the data is being propagated and sold without any permissions asked or received.

This legislation and regulation, if it is really going to be effective, should be addressing those misuses directly; **An "Opt Out" button, no matter how available, is like holding up a hand to stop a tidal wave.** You, as an individual are going to be washed away...

Message

From: Brent Blackaby [redacted]
Sent: 12/6/2019 9:00:23 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Crid Yu [redacted]
Subject: CCPA written comment
Attachments: 20191206 Confidently CCPA written comment.pdf

Attached please find a written comment on the proposed CCPA implementation regulations from Brent Blackaby and Crid Yu at Confidently.com.

Please email or call us at [redacted] with any questions or concerns.

Thank you,

Brent Blackaby
Confidently.com

Written Comment
on Proposed CCPA Regulations

Submitted by:
Brent Blackaby & Crid Yu
Confidently.com

December 6, 2019

We are submitting this public comment as two California residents who deeply care about our own online privacy, as well as co-founders of a new company called Confidently, building products and services to help consumers take full advantage of the new privacy rights they've been granted here in California. Our aim is for consumers to fully realize their rights to their privacy.

We applaud the California Attorney General's office for putting forth a comprehensive set of regulations to guide the implementation of the California Consumer Privacy Act (CCPA). Thanks to the CCPA and these regulations, consumers will have powerful new rights to help them manage their personal data and enhance their privacy.

Our own consumer research shows that consumers are very interested to have the ability to 1) access their data, 2) delete their data, and 3) instruct companies to not sell their data -- and to do all these things not just with a handful of businesses, but with all the businesses who may have their data, whether they are customers or not. That's potentially hundreds or thousands of businesses.

We are very optimistic that the legislation address key consumer concerns, but our biggest concern is scalability: how consumers can execute all of these access, delete, and do not sell requests across their entire digital portfolio of business relationships.

Based on recent experience from the GDPR in Europe, most of the EU privacy officers we've talked to report receiving only a handful of data access requests every week, even while serving millions of consumers who report, in survey after survey, that they are very concerned about their privacy. We believe this is because the process for consumers to act on their rights is, in many respects, too arduous and arcane. In the EU data requests are often done by writing an email to a company's Chief Privacy Officer who can then require additional data, clarification, etc. The reality is that one would have to really persist, and perhaps have legal counsel, to be able to actually complete just one data request.

This is compounded by the number of requests a consumer has to do to make meaningful impact to their privacy. Based on our own research, we estimate that for a typical consumer there are 50 or so businesses who have significant amounts of their data (those places where they are actual customers with login accounts), and hundreds if not thousands of businesses who have some of their data (most of whom consumers may not even know about). From our observation, it is daunting for most consumers to complete even one request -- let alone the hundreds or thousands necessary to secure their privacy across every digital relationship.

The key to success for the CCPA will be **both** ensuring appropriately rigorous standards for verification and authentication **and** making it easy enough for consumers to participate across their entire portfolio of digital relationships. Ultimately the success of the CCPA relies on consumers taking up their new privacy rights at scale. To effectively manage their privacy, consumers don't want to just act on their rights in one or two places — they want to do it everywhere.

Fortunately, the CCPA has built on the GDPR and addressed some of its shortcomings -- including by defining a global webform requirement for making "do not sell" requests. But Delete and Access requests will still be very laborious, even for companies where consumers are not customers and do not have accounts. Therefore, our comments largely focus on the question of consumer accessibility.

To that end, we would suggest further clarification of these regulations to make it easier for consumers, on their own or through a trusted third-party service that they designate, to submit verifiable requests — especially to companies where they are not customers and the standard for authentication or verification may not be as high.

Specifically we recommend:

VERIFICATION (§999.323, §999.325): Especially with respect to Access or Delete requests where a user is not a customer and is just trying to see/delete the marketing prospect data that a company has collected on them, we suggest developing a standard set of documentation for verifying a request, across all businesses -- for example, a scanned copy of drivers license & utility bill, with full name, mailing address, phone, and email address; or even just a device ID, for example, in situations when full contact info isn't collected by a business, but a user's digital "fingerprint" has been collected..

This will make it easier for consumers to Access or Delete their data with multiple businesses in a standard, verifiable way -- rather than figuring out the unique requirements of each business. Because consumers are not customers, and do not have accounts in these cases, we believe a "reasonable degree of certainty" is the appropriate standard as there should usually not be sensitive personal information involved for non-customers.

Additionally, we suggest giving consumers' authorized agents the option to take on more of the verification burden themselves, before passing "pre-verified" delete/access requests along to businesses, to streamline the authentication process. If agents can be empowered to use a third-party verification service to verify the identity of their customers, and then submit pre-verified requests along to businesses, that could reduce the authentication burden for both businesses and consumers at scale.

AGENT AUTHORIZATION (§999.326): We suggest defining a standard, pre-approved document or process that will enable agents to present their authorization from an end user, to improve confidence from businesses, consumers, and agents that these authorizations are valid. Our suggestion would be a standard templatized document, signed by the consumer either physically or with a digital signature, authorizing that agent to make Delete, Access, and Do Not Sell requests on their behalf.

In the case of businesses where a consumer is not a customer, this authorization document could be sent alongside the standard consumer verification documents (suggested above), to facilitate the receipt and processing of valid Access and Delete requests. We do not believe that consumers should have to re-verify their identity in those cases.

PARTIAL DELETE (§999.312(d), §999.313(d)(7)): We suggest clarifying that consumers have the right to ask a business to delete some, but not all, of their data, in the very first request (not in response to a business' reply to that request as suggested in §999.313(d)(7)). For example, we believe consumers should be able to ask to delete some of the most sensitive personal information that a business may have collected on them (e.g., Social Security Number, credit card number), but keep the rest of their data intact. We suggest there should be a standardized format for this request to be performed, so a consumer does not need to figure out how each business handles these kinds of partial delete requests differently.

In addition to the suggested amendments to the regulations we have suggested above, there are areas where we seek more clarification:

DEFINING "USER-ENABLED PRIVACY CONTROLS" (§999.315(c)): Confidently is developing a web application to help consumers manage their personal data and privacy at scale. While it will not be a browser extension per se, it will be a subscription service where consumers will clearly sign up and demonstrate their intent for us to execute dozens of Do Not Sell, Delete, and Access requests on their behalf. This will be a technology product, accessed via the internet (desktop or mobile device) to act on the consumer's behalf, as if the consumer is making these requests directly. So we assume that a product like ours would fit under this definition of User-Enabled Privacy Controls, but would appreciate any clarification along these lines.

DELETING IP ADDRESS OR MOBILE AD ID (§999.323): If a consumer wants to delete their IP address, browser cookie, or mobile ad ID — and any associated data collected along with it — from a business' database, they may not have any more data other than that particular data point to verify that legitimate request. How can a consumer demonstrate the validity of that

Access or Delete request without supplementary/corroborating info? In that case, should the business assume that it is legitimate unless they can prove otherwise?

***

Thank you very much for drafting these CCPA implementation regulations that will allow consumers to better manage their privacy with all of the businesses that have collected their data -- and thank you for reviewing this written comment.

Message

From: Jessica Lee [redacted]
Sent: 12/7/2019 12:56:01 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: [redacted]
Subject: CCPA_ Comments to Proposed Draft Regulations - Submitted by Jessica Lee
Attachments: AG Comments .pdf

Attached.

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, C A 90013

Dear Attorney General Becerra:

My name is Jessica Lee. I am a partner at the law firm Loeb & Loeb LLP and the Co-Chair of its Privacy, Security & Data Innovations practice group. Our clients include advertisers, agencies, publishers and adtech companies. I am writing to provide comments on the California Office of the Attorney General's ("OAG") proposed regulations implementing the California Consumer Privacy Act ("CCPA"). I am not writing on behalf of any one client, or on behalf of other members of my firm, but in my own capacity as legal counsel to a number of organizations who are working diligently to prepare for January 1st.

Our clients respect the law and the privacy rights of their consumers/users. However, the draft regulations, released as companies were in the process of building out their compliance processes, have introduced a number of new obligations, which in some cases exceed the scope of the statute. Companies are now struggling to understand how and when to implement these new requirements. While the OAG has provided some clarity and helpful guidance in some areas, several sections of the regulations raise new questions and create implementation challenges that will require time to address.

To be clear, I offer these comments in an effort to help the OAG create a final set of regulations that provide the clarity needed for businesses to implement, and for consumers to receive the full benefit of, the protections of the law.

I. Delay the Effective and Enforcement Date of the Regulations until January 1, 2021

The draft regulations, which I understand are on track to become final in early 2020, impose additional obligations on businesses which exceed the scope of the CCPA. Obligations to provide notice of an opt-out to third parties that have received data in the previous 90 days, to honor browser signals, and the significant reporting obligations, as examples, are obligations that are not currently considered in the text of the statute. These obligations each require different technical and administrative processes to be developed, operationalized, and made auditable to confirm compliance. These are not impossible tasks, but they cannot be implemented overnight. Companies will not know which of these obligations will be included in the final regulations, or whether there will be material updates to these requirements following this round of comments. Particularly for mid-size companies who have limited resources and staff to devote to this process, the decision of whether and when to implement these regulations is a difficult one. When these regulations become final, companies may have as little as 4 months (if that) to implement changes to a process that they have been developing for over a year. If we look to the EU as an example, companies were given two years to comply with its requirements. Delaying the enforcement of these regulations for six months should not be an unreasonable request. While we appreciate that the OAG has expressed an intent to avoid "gotcha" cases and to work with companies who are using good faith efforts to work towards compliance, if the regulations become effective before companies have a reasonable time to address them, companies will face significant risk from the plaintiffs bar, which is eagerly awaiting the effective date of the CCPA and the regulations to bring their own "gotcha" claims. I testified in front of the Senate Judiciary Committee in March of this year about the steps companies took to comply with the GDPR and the steps that will be needed to comply with the CCPA.[1] As I stated then, these laws require significant shifts in how companies organize, store, and manage their data. I am not arguing against all of these requirements; but I think it's important to understand the real work that companies have to do in order to comply with them.

II. Streamline the Notice Requirements to Avoid Notice Fatigue and Ensure Helpful Information is Provided to Consumers.

[1] https://sd19.senate.ca.gov/news/2019-03-04-sen-jackson-convene-hearing-data-privacy

Article 2 of the draft regulations has created some confusion regarding the notices a company is expected to provide the consumer. Section 999.305 refers to a "notice at collection", Section 999.306 refers to the "notice of an opt-out of sale of personal information," and Section 999.308 refers to a "privacy policy," which must be posted online using the word "privacy." As written, the draft regulations suggest that a company that "sells" personal information may have at least three notices on its website - a notice of collection, a privacy policy, and a do not sell link. If a company offers financial incentives, or uses the DAA AdÇhoices icon for interest-based advertising, that number rises to 5 links. That is between 3 and 5 separate notices consumers will be required to navigate to get information about how their information is used and to exercise their rights.

As written, Article 2 is at risk of creating consumer notice fatigue. At minimum, I recommend clarifying that the notice required in Section 999.305 can be provided in the privacy policy referenced in section 999.308, rather than requiring a separate link. A link labeled "Your Privacy Rights," which takes the consumer to a page that contains the privacy policy with easy navigation at the top of the page to the information required in Section 999.305 would satisfy the apparent objectives of the OAG.

III. Reconsider the Scope of the Financial Incentive Disclosures

I am concerned about the requirements of Section 999.307(b)(5)(a), which include the obligation to provide a good faith estimate of the value of the consumer's data that forms the basis for incentive and the description of the method used to calculate the value of the consumer's data. This requirement raises a number of concerns. It is difficult for most companies to calculate on an individual user basis the value of one consumer's data In many cases, an individual's data is worth pennies to a company; instead, it is the value of having data from many consumers that is valuable (a car company doesn't want to sell one car, they want to sell millions of cars). The numbers, even if they could be provided, may not align with the incentive, which would be designed in encourage large numbers of individuals to participate, not just one. The likelihood of the average consumer understanding - or taking the time to dive into - the specific details of the business of online advertising seem slim. A business could outline the various models - whether the are paid based on impressions, or conversions, or some other metric, - but if the goal is to provide consumers with meaningful information, this doesn't seem like the best path.

I am also concerned about the language of Section 999.307(b)(5)(b), which require a business to disclose the method used to calculate that value. This information is proprietary to each company and is less likely to be used by consumers than it is by businesses looking to gain insights for negotiation tactics and a competitive business advantage.

I understand the desire to help the consumer make an educated decision about whether the incentive is worthwhile; however, the suggested disclosures will likely create more confusion and may act as a disincentive to companies who are concerned that can't provide a valuation for data at an individual level or that are concerned about the risks that this information will be misused by competitors.

Instead, consider revising 999.307(b)(5) to read: An explanation of why the financial or price or service difference is permitted under the CCPA, including: (a) for differences in price or service, a meaningful description of why the business cannot provide the same price or level of service without access to the consumer's personal information; and (b) for financial incentives, a meaningful description of how the business benefits from its ability to collect, use or sell the consumer's personal information and how it determined that the financial incentive offered was a suitable exchange.

IV. Remove the Requirement for a Business to Treat an Unverified Request as an Opt-Out of Sale

Section 999.313(d)(1) requires businesses who cannot verify the consumer's identity to treat a request to delete information as a request to opt-out of a sale of that information. There are a few concerns with this. First, it violates the consumer's choice. To the extent that a business "sells" information, a consumer that chooses to opt-out of that sale, can use the business' do not sell link. Forcing businesses to treat an inability to verify a deletion request as a de facto opt-out request overlooks the fact that if the consumer would like to opt-out of a sale, that choice is already available to them. If a consumer did not choose to opt-out of sale, he or she should not be forced to do so. Where consumers are benefiting from a financial incentive or access to certain prices or services because they have not opted-out of sale, the request to delete all or a portion of their personal information would result in them losing out on these benefits.

Second, a business that does not have the information required to facilitate a deletion request (i.e. does not have the information required to identify the consumer with any reasonable degree of certainty), may similarly not have the information required to facilitate the opt-out request.

I am asking the OA to delete the last sentence of Section 999.313(d)(1).

V. Remove the Requirement for Businesses to Respond to Browser Signals Until a Uniform Standard and Protocol is in Place

Section 999.315(c) introduces a new requirement in the CCPA - to treat browser-based signals as an opt-out. Currently, there is one industry developed standard for browser based signals developed by the W3C, as well as various browser-based controls. Mandating that businesses treat all of these signals as a blanket opt-out of sale is a requirement that is not reflected in the text of the CCPA and which also introduces the possibility of "signal mayhem" that takes choice away from consumers (who may have default browser settings that don't reflect their intentions), and puts it in the hands of other entities who may create default browser settings designed to increase the browser's position and control of data to the detriment of the other businesses in the online advertising ecosystem. In addition, there is no clarity as to how a browser signal would interact with a consumer who has opted-in for a financial incentive, or who desires to make a more granular selection regarding their opt-out rights.

I suggest deleting this requirement until there is clear guidance on how browser signals should be selected by companies and read by businesses. The new CCPA ballot initiative proposes browser-based opt-outs and would become effective in 2021. Consider using the time between now and then to more fully develop guidelines around the use of browser-based privacy controls, rather than introducing it now when it may create more mayhem than consumer choice.

In closing, I would like to emphasize that businesses are spending a lot of time and money to prepare and adapt to these new regulations. For many, despite their efforts, there are still more questions than answers. In some cases, the technology required just doesn't exist or is still being developed. Data-driven advertising allows many of our clients to provide content to consumers for free. This ad-supported internet model is not perfect, but it is the means through many, particularly those without the financial resources to pay for content, can access the Internet. Consumers should be given an opportunity to understand this dynamic and make meaningful choices about how they interact online. I think my suggestion will help push us in that direction.

I look forward working with the OAG and I hope the office will be amenable to helping companies work through these challenges, rather than punishing good faith efforts to comply. I appreciate the opportunity to provide these comments. Please contact me with any questions.

Best,

Jessica B. Lee
Co-Chair, Privacy, Security & Data Innovations
Loeb & Loeb LLP
[redacted]

Message

From:	Elizabeth Bojorquez [redacted]
Sent:	12/6/2019 10:23:20 PM
To:	Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC:	Jacqueline Kinney [redacted]
Subject:	CCTA Comments on CCPA Regulations
Attachments:	CCTA Comments to AG on CCPA 12-6-19 FINAL.pdf

Good Afternoon,

The California Cable and Telecommunications Association submits the attached comments regarding the proposed regulations for the California Consumer Privacy Act.

Thank you,

Elizabeth Bojorquez
California Cable & Telecommunications Association
1001 K Street, 2nd Floor
Sacramento CA 95814
(916) 446-7732 (office)
[redacted]

CCTA
California Cable & Telecommunications Association

Carolyn McIntyre
President

1001 K STREET, 2ND FLOOR
SACRAMENTO, CA 95814

[redacted]

December 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator 300 S. Spring St.
Los Angeles, CA 90013

Submitted via electronic mail to privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act Proposed Regulations

The California Cable and Telecommunications Association ("CCTA") submits these comments pursuant to the Notice of Proposed Action ("NOPA") published October 11, 2019, by the Attorney General ("AG") to implement the California Consumer Privacy Act ("CCPA").[1]

CCTA is a trade association of member companies that provide video, voice, and Internet service to millions of customers across California. At the outset, CCTA emphasizes that our member companies are committed to protecting customer privacy and currently operate subject to a variety of existing federal and state privacy laws and regulations. Some CCTA members also are subject to the European Union's General Data Protection Regulation ("GDPR"). CCTA has been actively engaged in legislative activity related to the CCPA, participated in the AG's pre-rulemaking public hearings in January and February, and filed preliminary comments with the AG on March 8, 2019. CCTA's goal has been, and continues to be, working with policy makers and learning from our cable industry customers to ensure that the CCPA is workable and will effectively improve privacy protections.

CCTA's comments include Section I, an overview of legislative direction in the Administrative Procedure Act and CCPA to adopt regulations with the goal of minimizing burden on business; Section II, recommended revisions to proposed regulations that are CCTA priorities; and Section III, a review of shortcomings with the AG's reasons for its proposals and with the cost analysis, along with an explanation of how CCTA's recommended revisions address these shortcomings.

[1] The AG's NOPA and all related CCPA rulemaking information is at https://oag.ca.gov/privacy/ccpa.

I. **CCPA and Administrative Procedure Act Require that AG Regulations Be within the Scope of and Consistent with the CCPA, Necessary to Effectuate the CCPA Purposes, and Minimize Burdens on Business.**

CCTA's comments and recommended revisions to the AG's proposed regulations are based on key provisions of the Administrative Procedure Act ("APA")[2] that govern the scope of agency rulemaking authority and standards for determining whether regulations are legally valid. These include the following provisions of the Government Code:

> Section 11342.1 … Each regulation adopted, to be effective, shall be ***within the scope of authority*** conferred and in accordance with standards prescribed by other provisions of law.
>
> Section 11342.2 Whenever by the express or implied terms of any statute a state agency has authority to adopt regulations to implement, interpret, make specific or otherwise carry out the provisions of the statute, no regulation adopted is valid or effective unless ***consistent and not in conflict with the statute*** and ***reasonably necessary to effectuate the purpose of the statute***. (emphasis added)

The CCPA expressly directs the AG to adopt regulations to implement the CCPA, including regulations that the AG is *required* to adopt to address issues enumerated in Civil Code Section[3] 1798.185(a), and any "*additional regulations as necessary* to further the purposes" of the CCPA, as provided in Section 1798.185(b). Thus, under both the APA and the CCPA, it is necessary to consider the purposes of the CCPA, as reflected in the statutory language and legislative history. As a starting point, the legislative findings adopted with enactment of AB 375 highlight the Legislature's specific concern with consumer harm caused by large data mining firms.[4] These findings describe the consumer harms that the CCPA is intended to prevent as follows:

> 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.[5]

The CCPA reflects legislative intent to prevent these potential consumer harms in two ways: by (1) granting consumers rights to understand and manage the personal information a business collects, sells, uses or discloses, and (2) ensuring that the process for consumers to exercise these rights does not create additional privacy risks. To ensure that additional privacy risks do not arise from consumers exercising their rights, the Legislature directed the AG to specify requirements for a business to verify any consumer request to access, delete, sell, or disclose personal information. Furthering the legislative intent to prevent consumer harm must be a touchstone for each regulation the AG adopts.

[2] Government Code Sections 11340 to 11361.

[3] All further section references are to the Civil Code, unless otherwise specified.

[4] AB 375 (Chau 2018), Ch. 55, Stats. 2018, Sec. 2(g).

[5] Id., at Sec. 2(f).

The APA further requires an agency to state, in an Initial Statement of Reasons ("ISOR") and final statement of reasons, why each proposed regulation is reasonably necessary to address a specific problem posed by the authorizing statute.[6] The public benefits of the regulation, and alternatives that may be less burdensome and equally effective in achieving the purpose, must be considered.[7] In addition, the rulemaking agency is required to consider potential adverse economic impact of each regulation on California businesses and individuals, with the goal of ***"avoiding the imposition of unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements."***[8]

In addition to the legislative purpose and general APA requirements, specific directives in the CCPA are highly relevant to determining what AG regulations should be adopted to implement, interpret, or otherwise carry out the provisions of the CCPA. For example, the CCPA provides that it is intended to supplement existing federal and state law and that it should be harmonized with other laws when possible, while also acknowledging that federal law may preempt or create conflicts with the CCPA.[9] Other provisions emphasize ensuring that the rights afforded to one consumer do not result in harm to another. Section 1798.145(j) provides that the rights afforded to consumers and the obligations imposed on businesses by the CCPA "shall not adversely affect the rights and freedoms of other consumers." Section 1798.145(k) similarly provides that these CCPA rights and obligations shall not apply to the extent that they infringe on noncommercial free speech activities protected by the California Constitution.

Moreover, despite the CCPA's affirmative grant of rights to consumers and imposition of obligations on businesses, Section 1798.145 contains a long list specifying what these obligations shall *not* do and to which they shall *not* apply. These include, for example, not restricting a business's ability to comply with federal, state, or local laws, and not restricting a business's ability to collect, use, retain, sell, or disclose consumer information that is deidentified or aggregated.[10] The CCPA also expressly directs the AG to give consideration to "obstacles to implementation" and "the goal of minimizing the administrative burden on consumers" and "the burden on business."[11]

The Legislature acknowledged the potential overwhelming burden on businesses of operationalizing the CCPA by providing for flexibility given the "complexity and number" of consumer requests and in the event of a business receiving "requests from a consumer [that] are manifestly unfounded or excessive."[12] The Legislature's recognition of the complexity of the CCPA and uncertainty about precisely what conduct the CCPA actually requires also is evident in Section 1798.155, which authorizes any business or third party to seek guidance from the AG on how to comply with the CCPA.

[6] Government Code Section 11346.2(b)(1).

[7] Id.

[8] Government Code Section 11346.3(a) (emphasis added).

[9] See Section 1798.196 (the CCPA "is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution"); and Section 1798.175 (the CCPA "is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information…[and] should be construed to harmonize" with other privacy laws).

[10] Section 1798.145(a).

[11] Section 1798.185(a)(1), (2) and (7).

[12] Section 1798.145(g)(3).

Thus, CCTA's comments urge the AG to consider all of these provisions that require it to balance the goal of protecting consumers' privacy with minimizing the imposition on business of implementation obstacles, new cost or other burdens, and uncertainty, as well as the APA's general requirement that agency regulations be "reasonable."[13] Only such a balanced approach can faithfully achieve the CCPA's purposes consistent with the APA and other applicable requirements noted above.

II. Recommended Revisions to Proposed Regulations

A. Request to Delete: Proposed regulation 999.313(d)(1)'s requirement that a business convert an unverified request to delete into an opt-out request needs revision to ensure consistency with CCPA's protection of consumer choice and the statutory scheme requiring a business to act on a consumer request only after verification.

The AG's proposed regulation 999.313(d)(1) relating to consumer requests to delete personal information provides as follows:

> "(d) Responding to Requests to Delete
> (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***." (emphasis added)

CCTA supports two aspects of this proposed regulation – the authorization of a business to deny a consumer's request to delete if the requester cannot be verified, and the requirement that the business inform requesters that their identity cannot be verified. These provisions appropriately implement the CCPA's strict requirements for verification of consumer requests and are consistent with the overall statutory purpose of enabling consumers to control their personal data. However, CCTA objects to the requirement in proposed regulation 999.313(d)(1) that a business must treat any unverified request to delete as a request to opt out of sale, the latter of which is a wholly distinct right already afforded to consumers under the CCPA.

While the CCPA grants consumers separate rights (1) to request deletion of their personal information and (2) to opt out of the sale of their personal information, the plain language of the CCPA does not require a business to convert an unverified request to delete into an opt-out of sale request. Nor does the ISOR cite any statutory basis for this requirement. The ISOR in support of 999.313(d)(1) provides as follows:

> "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***

[13] See Government Code Sections 11342.2 and 11346.3(a).

> ***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."[14]

The ISOR asserts that a requirement to convert an unverified request to delete into an opt-out request is necessary to "instruct businesses on what they should do when they cannot verify the identity of the consumer." But this falls far short of establishing that this conversion requirement is necessary to effectuate the statutory purpose of the CCPA, which is what the APA requires. In fact, the CCPA already directs a business what to do, and this proposed regulation is squarely *inconsistent* with the CCPA on this count. Section 1798.140(y) expressly provides that "[a] business is not obligated to" comply with a consumer request "if the business cannot verify" "that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf." If a business has been unable after diligent effort to verify the identity of an individual making a deletion request, that business has no basis for assuming that same individual is who he says he is for purposes of applying an opt-out of sale. In fact, the CCPA text quoted above directs businesses to presume the *exact opposite*. Proposed regulation 999.313(d)(1) is thus inconsistent with both the plain language of the CCPA and proposed regulation 399.315(h), which recognizes the potential for fraud and associated consumer harms with acting on unverified requests to opt out.[15]

But even assuming *arguendo* that the requesting individual *is* who he says he is, the proposed regulation still makes an invalid assumption – namely, that a consumer who seeks to delete personal information and is denied would want to opt out of all sale of his personal information instead. That is surely not the intent of *every* consumer who submits a request to delete.[16] If it were, the statute would have included this default to an opt-out of sale in cases of unverified deletion requests, or perhaps even mandated that all *verified* requests for deletion *also* be treated as requests to opt out of sale, based on a similar assumption that any consumer who asks for his data to be deleted must also want to opt out of the sale of his data. The CCPA does neither. Instead, the CCPA maintains deletion requests and opt-out requests as *distinct* rights for the *consumer* to pursue *separately* if and as he wishes. In this case, if the actual consumer already opted out of the sale of his personal information, then the last part of proposed regulation 999.313(d)(1) is not needed, and if the consumer has *not* opted out of sale, the rule would be mandating the execution of a choice for him that the consumer has indicated he does *not* want. In either case, the assumption underlying proposed regulation 999.313(d) is unfounded and inconsistent with the statutory requirement that these rights must be pursued independently *by the*

[14] ISOR at 19 to 20 (emphasis added).

[15] ISOR at 25 to 26.

[16] Accordingly, the ISOR also is wrong in claiming that this subdivision benefits consumers because not all consumers want a request to delete treated as a request to opt out.

consumer himself.

The statutory requirement in Section 1798.135(a)(5) that a request to opt out of sale must remain in effect for 12 months also mitigates against the proposed regulation's assumption of consumer intent. The effect of a consumer's decision to opt out continues for 12 months and can be reversed only by another affirmative action by the consumer. This 12-month duration of the opt-out decision makes it especially inappropriate that the decision be made for a consumer based on an unsupported assumption by a government agency.[17]

Finally, proposed regulation 999.313(d)(1) is also unreasonable because, if a business cannot verify the consumer making the request to delete, that lack of verification almost certainly would significantly impede the ability of a business to accurately associate the consumer with information in its system in order to treat the request as a request to opt out.[18]

Thus, CCTA recommends that 999.313(d)(1) be revised as follows:

> "(d) Responding to Requests to Delete
> (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~~shall 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~~."

B. Do Not Sell Global Opt-Out of Sale: Proposed regulation 999.315 needs revision because a global opt-out is not required by the CCPA, is unreasonable given that compliance is not technically feasible, and imposes unworkable obligations on business without furthering the purposes of the CCPA.

CCTA appreciates that proposed regulation 999.315(b) recognizes that flexibility is needed for offering methods for submitting requests to opt out of sale given the wide range of business practices and relationships with consumers. However, CCTA objects to the requirement for a "global option to opt-out of the sale of all personal information" as referenced in subdivision (d) of 999.315. Such a global opt-out is not required by the CCPA and in many cases is not technically feasible for companies that engage in varying types of "sales" across different online or offline channels.

For example, subdivision (c) of proposed regulation 999.315 requires that "[i]f a business collects personal information from consumers online, the business shall 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 [opt-out]

[17] *See also* ISOR at 26 (discussing proposed regulation 999.316).

[18] The proposed regulation is also flawed in that it says the business "may" deny the request to delete if it is unverified. That conclusion should not be discretionary and is contrary to the actual text of the CCPA; rather, given that Section 1798.105(c) and 1798.140(y) impose a strict requirement to verify a requestor's identity before a request to delete is processed, in cases where such identity *cannot* be verified, the business should be precluded from deleting the personal information at issue. Accordingly, in order to be consistent with the CCPA, the regulation should instead state that the business "shall" (not "may") deny the request in such cases.

request …." However, while a business may follow opt-out cookies on browsers and other such user-enabled signals for opt-out, and while such opt-outs may prevent future sales of a consumer's personal information through that online channel, the business very well may not even know that the consumer exercised the opt-out, the identity of the consumer, or have any way of contacting him, as this is a browser-based control that may not be tied to any personally identifying information. As a result, the business would be unable to implement an opt-out for the sale of the consumer's other personal information across other channels. To attempt to do so would actually mean that businesses would be forced to collect *more* personal information from a consumer (*e.g.*, their name, address, or email address) before the initial opt-out in order for a broader opt-out to be executed. That would create a worse consumer experience and be contrary to key goals of the CCPA.[19] Proposed regulation 999.315(c) seems to acknowledge this reality when it says that the browser-based opt-out shall be deemed an acceptable method of opt-out pursuant to Civil Code section 1798.120 "for that browser or device, or, ***if known***, for the consumer." (emphasis added) Given that, in many cases, the identity of the consumer would *not* be known, the global opt-out requirement of proposed regulation 999.315(d) is unworkable and should be revised.

Another example reinforces this conclusion. In cases where a consumer provides his email address or other identifying information, the business will opt the consumer out of the sale of his personal information for most channels, but as there is no technical way for the business to use that email address or other such contact information to effectuate an opt-out of the "sale" of that consumer's personal information in the online context – *i.e.*, by changing a setting in a cookie or otherwise triggering an opt-out switch on a DAA or other opt-out flag – that means that the business would *not* be able to opt the consumer out of certain online sales of personal information.

As a final example focused solely on online opt-outs, a website may have both Google Analytics and Adobe Analytics/Omniture cookies and those companies can use the information collected from the cookies to create their own analytics reports. While both Google and Adobe offer their own opt-outs that consumers can execute, and while the website operator in this example can aggregate and present these various opt-out options to consumers on a landing page, the website operator cannot technically trigger the Adobe opt-out if a consumer executes the Google opt-out or vice versa, nor can it combine the opt-outs collected by those two companies with other opt-outs the business does control or with other cookie opt-outs.

For these reasons, CCTA recommends the following changes to subdivision (d) of proposed regulation 999.315(d) to make it consistent with the CCPA and to reflect how opt-outs technically and actually work in the marketplace:

> "(d) In responding to a request to opt out, a business may present the consumer with the choice to opt-out of sales 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; provided, however, that the business must implement a requested global opt-out of the sale of the consumer's personal information across different channels only to the extent that such opt-outs (1) are user-enabled as opposed to default settings by a browser or other technology; (2) are technically feasible using readily available,

[19] It also would be contrary to other proposed AG regulations, notably the determination that verification is not required for a business to implement opt-out requests due to the "importance of a minimally burdensome verification procedure to foster the use of privacy services that empower consumers." ISOR at 25 (discussing subdivision (h) of proposed regulation 999.315).

commercially reasonable methods; and (3) may be implemented by the business without having to collect additional personal information from the consumer."

C. Service Provider Sale Exemption: Proposed regulation 999.314(c) needs revision to be consistent with the CCPA definitions of "service provider," "sale," and "business purpose."

Proposed regulation 999.314(c) provides as follows:

> "(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. A service provider may, however, 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 detect data security incidents, or protect against fraudulent or illegal activity."

CCTA's concern with this proposed regulation is that it contravenes the CCPA in several ways by severely reducing the scope of responsibilities and functionalities that may be undertaken and performed by service providers under the plain language of the CCPA. The problem relates mostly to the second sentence of this proposed regulation, which seeks to impose significant restrictions on a service provider's use of data even if such uses would be well within the business purposes for which the business contracts with that service provider. Specifically, this proposed regulation allows a service provider to combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, *only* "to the extent necessary to detect data security incidents, protect against fraudulent or illegal activity." That significant limitation is squarely at odds with the CCPA for at least three reasons – namely, it conflicts with the CCPA's definitions of "service provider," "sale," and "business purpose."

First, the CCPA defines service provider as follows:

> "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information ***for a business purpose pursuant to a written contract***, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than ***for the specific purpose of performing the services specified in the contract for the business***, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than ***providing the services specified in the contract with the business***.[20]

The highlighted language above makes clear that a business may hire a service provider and share personal information with that service provider which it may then use for: (1) "a business purpose pursuant to a written contract," and (2) "the specific purpose of performing the services specified in the contract for the business." These clear statutory provisions and

[20] Section 1798.140(v) (emphases added).

authorizations would allow a service provider hired by both Business A and Business B to combine personal information that the service provider receives from these businesses, so long as such combination is done to perform the business purposes and provide the services specified in the contracts with Business A and Business B. This may, in fact, be precisely what a business hires a service provider to do for it. For example, Business A may want a service provider to receive Business A's data about its customers and combine it with data the service provider has about consumers from other businesses, so that Business A can learn about trends in the marketplace, consumers' use of various products and services, what consumers are interested in, etc. In this role, the service provider is not disclosing the personal information of any particular consumer or business to another business; rather, it is using all of that information internally to perform analytics and then report back to Business A regarding aggregate trends and information that will assist the business to improve its products and services and to better serve its customers and consumers more generally. This is commonplace usage of service providers across various industries that the CCPA authorizes and that therefore must be permitted by the AG's regulations, especially since it is beneficial to consumers and businesses without reducing privacy protections.

By contrast, proposed regulation 999.314(c) would limit all service providers to combine such data *solely* "to the extent necessary to detect data security incidents, protect against fraudulent or illegal activity." That severe limitation is nowhere authorized by the CCPA and in fact is contradictory to it in that it dramatically reduces the functions that the statute authorizes service providers to perform for businesses, thereby substantially impairing the ability of businesses to improve their products and services, which will only harm consumers.

Second, the proposed regulation is inconsistent with the CCPA's definition of "sale." Specifically, the CCPA expressly states that it is *not* a sale triggering the law's opt-out requirement if:

> "(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
>
> > (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.
> >
> > (ii) ***The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose***.[21]

The emphasized language makes clear that a service provider *can use* internally or *even sell* a consumer's personal information that it receives from a business so long as it is "necessary to perform the business purpose" for which the business hired the service provider. Given this express statutory authorization to use or even further sell a consumer's personal information, proposed regulation 999.314(c) cannot limit a service provider's internal use and combination of a consumer's personal information as long as such use/combination is "necessary to perform the business purpose" specified in the written contract between the business and the service provider.

Third, the proposed regulation limiting the combination of personal information for only detection of security incidents, fraud, or illegal activity is inconsistent with the CCPA's definition of business purpose, which provides as follows:

[21] Section 1798.140(t)(2)(C) (emphasis added).

> (d) "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:
>
> > (1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
> >
> > (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
> >
> > (3) Debugging to identify and repair errors that impair existing intended functionality.
> >
> > (4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
> >
> > (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.
> >
> > (6) Undertaking internal research for technological development and demonstration.
> >
> > (7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.[22]

In contrast to this broad statutory definition of "business purpose," proposed regulation 999.314(c) allows for the combination of data by the service provider *only* for a very narrow set of purposes – namely, to "detect data security incidents, protect against fraudulent or illegal activity." But that narrow set of purposes ignores a number of other activities and functions that are permitted by the CCPA definition of business purpose, including "internal research for technological development and demonstration," a very common practice that inures to the benefit of service providers, the businesses for which they provide services, and the consumers who ultimately get to use the resulting innovative products and services. The proposed regulation and the ISOR overlook the fact that the business purpose definition includes specific references to "or other notified purposes" and to "another operational purpose that is compatible with the context in which the personal information was collected"; these are significant provisions that must be given meaning in the AG's regulations. Failure to include a reference to the full range of business purposes that the statute allows service providers to perform for businesses would again be inconsistent with the CCPA and harm consumers.

[22] Section 1798.140(d).

CCTA would have no objection if the regulation sought to clarify that a service provider may not use personal information from Business A to combine it with data from Business B unless such combination is consistent with the business purposes for which Business A hired the service provider. But that is not what the proposed regulation says, and it therefore needs revision to make it consistent with the CCPA and to avoid constrictions on service provider activity that both protect consumer privacy and foster greater improvements in products and services that benefit consumers.

Thus, to ensure consistency with the CCPA and for the other reasons set forth above,[23] CCTA recommends revising proposed regulation 999.314(c) as follows:

> "(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. A service provider~~ may~~,~~ ~~however,~~ 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 perform the business purposes specified in the written contracts with such business ~~detect data security incidents, or protect against fraudulent or illegal activity~~."

D. Do Not Sell 90-Day Look-Back: Proposed regulation 999.315(f) needs revision because it exceeds the scope of the CCPA, is not necessary to effectuate the purpose of the CCPA, and imposes unreasonable and burdensome requirements on business with little if any additional privacy benefit for consumers.

The CCPA expressly provides that a business shall not sell the personal information of a consumer who has directed the business to not sell that information. As part of proposed regulation 999.315 to implement the CCPA's do not sell requirements, subdivision (f) provides as follows:

> "(f) 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."

This proposed regulation exceeds the scope of the CCPA because it is not required in the text of the CCPA, and the ISOR does not cite to any provision of the CCPA that directly requires subdivision (f). The ISOR asserts that proposed regulation 999.315(f) is "necessary" to further the purposes of the CCPA and that the burden on business with these requirements is outweighed by the benefit of giving consumers "greater transparency" as to which business holds their information.[24] The ISOR is incorrect on both counts. First, 999.315 is *not* necessary because the CCPA already contains a provision to address the transparency issue raised by this proposed regulation: Section 1798.115(d) states that "[a] third party shall not sell personal information

[23] CCTA's recommended revision deletes the last phrase of subdivision (c) because it is redundant given that the CCPA definition of "business purpose" includes "[d]etecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity" (Section 1798.140(d)).

[24] ISOR at 24.

about a consumer that has been sold to the third party by a business ***unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120***."[25] In other words, the statute *already* addresses the core concern that the ISOR claims it needs a new rule to address, namely that "consumers may not know the identity of the companies to whom businesses have sold their information in order to make an independent request."[26] Given this requirement in the CCPA, the consumers need not know all the third parties that receive their personal information from a business with whom the consumer has a relationship because (1) the consumer may opt out of the sale of any of his personal information by the business, and (2) Section 1798.115(d) requires any third party to provide notice and an opt-out choice to that same consumer before it may further sell any personal information of that consumer that the third party received from the business.

Second, the ISOR is incorrect that the burdens on business imposed by this proposed regulation are outweighed by the assertedly new transparency. For the reasons discussed above, the proposed regulation does not add any new transparency rights to consumers. As a result, the proposed regulation merely creates an additional burden on businesses without a corresponding consumer benefit. Moreover, the burdens associated with attempting to implement the requirements of this proposal would be enormous. Businesses would have to create entirely new operations for tracking and notifying third parties to whom they provide personal information within a particular timeframe and for specific consumers, as well as new mechanisms for contacting and notifying consumers to let them know when such third-party notifications have been completed. These are not simple processes; they are quite intricate, complex, and costly especially given the substantial volume of consumer transactions that businesses handle. The conclusions in the ISOR are broad and general and do not even acknowledge any of these specific business burdens or the practical difficulties of complying with subdivision (f). This lack of discussion of these burden and cost issues by the ISOR ignores the CCPA's clear direction that the AG consider "obstacles to implementation" and the goal of minimizing "the burden on business."[27]

Thus, CCTA recommends that proposed regulation 999.315 be revised by striking subdivision (f):

> ~~"(f) 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."~~

E. <u>Customer Notice and Privacy Policy: Proposed regulations 999.305 and 999.308 need revision to eliminate duplicative notice requirements that exceed the scope of the CCPA, do not effectuate the statutory purpose of ensuring consumers understand their rights, and imposes unreasonable burdens on business and frustrating new online "speed bumps" for consumers.</u>

The ISOR states that the AG is seeking to provide business with flexibility in providing

[25] Section 1798.115(d) (emphasis added).
[26] ISOR at 25.
[27] Section 1798.185(a)(1), (2), and (7). *See also* Government Code Sections 11346.2(b)(1) and 11346.3(a).

consumer notices in order to "best facilitate the comprehension of these notices."[28] Regarding the proposed regulations on consumer notice, the ISOR states:

> "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."[29]

While appreciating this intent, respectfully, that is not what the proposed regulation would achieve. As written, proposed regulation 999.305 mandates a complex and highly detailed "Notice at Collection" that is largely duplicative of information that proposed regulation 999.308 requires be included in a "Privacy Policy." Express terms of the CCPA do not authorize, let alone require, such duplicative notice to consumers, nor is such duplication necessary to effectuate the purpose of the CCPA; and indeed it contravenes the goals of minimizing burdens on business and consumers.

The CCPA's requirement for notice related to collection is in Section 1798.100(b), which provides as follows:

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

This plain language is clear that the CCPA does not require a notice precisely at the point of collection, but instead provides the option of providing the required notice "at or before" collection.

Section 1798.185(a)(6) requires the AG to adopt regulations to ensure that notices *required* by the CCPA are understandable and accessible:

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

Significantly, the CCPA does *not* require a business to have a privacy policy, and, in fact, expressly acknowledges that not every business may have a privacy policy. Section 1798.130(a)(5) provides:

> "1798.130(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

[28] ISOR at 43.
[29] ISOR at 43.

> **
> (5) Disclose the following information in its online privacy policy or policies ***if the business has an online privacy policy or policies*** and in any California-specific description of consumers' privacy rights, or ***if the business does not maintain those policies***, on its Internet Web site, and update that information at least once every 12 months….
> (emphasis added)

Similarly, Section 1798.135(a) requires information on do not sell links and related information in "[i]ts online privacy policy or policies ***if the business has an online privacy policy or policies***." (emphasis added)

Read together, the plain language of the CCPA is clear that the legislative mandate to provide notice "at or before" the point of collection of personal information could be met through a single privacy policy. If a business has a privacy policy that is accessible to a consumer "at or before" collection, nothing in the plain language of the CCPA requires a separate notice in addition to that privacy policy. Similarly, any business that does not have a formal "privacy policy" could meet the Section 1798.100(b) mandate for notice "at or before" collection with the information specified in proposed regulation 999.305. In this instance, the lack of a duplicative privacy policy would not be a violation of the CCPA because there is no statutory mandate to have a privacy policy. (Proposed regulation 999.308 also does not directly require a privacy policy, but requires information that should be *in* a privacy policy.)[30]

The Legislature could have, if it had wanted to, expressly required both notice "at or before" collection and in a privacy policy, but it did not do so. And the regulations the Legislature directed the AG to adopt in this area are carefully limited to regulations that "ensure that the notices and information that businesses are ***required*** to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer." (emphasis added) The CCPA grant of authority to the AG to draft regulations thus expressly limits the AG and does *not* authorize the AG to create a requirement for *additional* notices to consumers. Proposed regulations 999.305 and 999.308 are therefore beyond the scope of the AG's authority, and it is unlawful for the AG to enlarge the scope of the CCPA in this respect through regulation.

Nor is it necessary (or helpful to consumers) that the proposed regulations require detailed notice both at collection and in a privacy policy in order to effectuate the purpose of the CCPA. To the contrary, regulations that result in businesses bombarding consumers with excessive information is inconsistent with the CCPA's overarching statutory purpose of ensuring consumers have knowledge to choose how to manage their own personal information. It is well documented that consumers view the type of extra notices that would be required by proposed regulations 999.305 and 999.308 as confusing and annoying speed bumps that they must click through to get to the online content they desire.

For example, studies of the GDPR experience show that such repetitive privacy notices only compound consumer frustration no matter how well-intended notice requirements may be. Pop-up privacy notices have become omnipresent online after the implementation of the GDPR,[31]

[30] In the NOPA, the AG incorrectly refers to a privacy policy as "required" by the CCPA (NOPA at 8).

[31] A 2019 research paper by German and U.S. academics found that 62.1% of the 6,759 websites they studied now display cookie consent notices, a 16% increase from January 2018. (Degeling, Martin, Christine Utz, et al. "*We Value*

but consumers do not find them helpful, if they read them at all. As one report stated, "GDPR is perhaps best known as a bothersome series of rapid-fire pop-up privacy notices," which are creating "consent fatigue;" overall, consumers "have become blind to an avalanche of privacy pop-up notices."[32] Another report concluded:

> "[A]ll the GDPR has done is made people constantly need to click on annoying privacy and cookie notices that they don't read and don't find useful at all."[33]

Consumers also cite economic impacts from burdensome privacy notices that make websites inaccessible. As one analyst stated:

> "The reality is that many people, in order to save time, simply click "OK" on the never-ending stream of pop-ups and most everyone I spoke to confess that they just move on when unable to access the desired website."[34]

This loss of access can make or break a small business or a start-up. As reported by *Forbes*, Internet users who shared their experiences with the GDPR complained about frustration in being unable to access sites essential to their business:

> "[A business owner] relates how she can no longer read sites she uses to build up her business in the food industry, 'I have to move quickly to learn about how to make my startup work in a competitive market. When you figure in all the clicking through for every single web site, that adds up to time. And what do they say? Time is money.'"[35]

Put more bluntly by another analyst:

> "[A]ll we have is a massive law that has harmed startups, entrenched big companies, failed to protect privacy and just served to annoy most users."[36]

Consumer confusion, annoyance, and frustration in California would likely be even greater than with the GDPR because the AG's proposed regulations would mandate that these extra notices contain a significant amount of detailed information that would make the new Internet "speed bumps" even larger and more aggravating than anything consumers have experienced to date. In fact, at the AG's public hearing on the CCPA in Sacramento on December 2, 2019, one person testified that, in light of all the CCPA mandated information consumers will be receiving, he is offering a new subscription service through a website called confidently.com for consumers

Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy" (2019) at https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_04B-2_Degeling_paper.pdf.

[32] *"Europe's sweeping privacy rule was supposed to change the internet, but so far it's mostly created frustration for users, companies, and regulators,"* CNBC News (May 5, 2019) at https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html

[33] *"One Year Into the GDPR: Can We Declare It A Total Failure Yet?"* (May 24, 2019) TechDirt at https://www.techdirt.com/articles/20190521/17425842255/one-year-into-gdpr-can-we-declare-it-total-failure-yet.shtml

[34] Id.

[35] *"How Tech Culture Has Changed Since the GDPR,"* (May 5, 2019) Forbes at https://www.forbes.com/sites/julianvigo/2019/05/05/how-tech-culture-has-changed-since-the-gdpr/#39b3720a79b0

[36] *"One Year Into the GDPR: Can We Declare It A Total Failure Yet?"* (May 24, 2019) TechDirt at https://www.techdirt.com/articles/20190521/17425842255/one-year-into-gdpr-can-we-declare-it-total-failure-yet.shtml

to get outside help to manage their online privacy.[37]

Finally, proposed regulations 999.305 and 999.308 run counter to the express terms of the APA and CCPA directing the AG to minimize burdens on business and consider obstacles to implementation.[38] The proposed duplicative notice requirements also are at odds with the NOPA, in which the AG seeks alternative regulations to lessen burden on business, specifically asking for "[c]onsolidation or simplification" of compliance requirements.[39] Moreover, the ISOR discussion of customer notice alternatives that the AG considered and rejected relate only to the manner of presentation and plain language of customer 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."[40]

Nothing in this excerpt or other portions of the ISOR reflect that the AG considered the alternative of meeting notice requirements solely through a company's privacy policy, which the CCPA clearly contemplates. The record from pre-rulemaking activities includes such recommendations to the AG, but the ISOR does not discuss them.[41] As noted above, the ISOR does state the AG's intent to ensure consumers understand their rights under the CCPA, but then only focuses on format and presentation of the notice to achieve this goal.

In short, proposed regulations 999.305 and 999.308 are neither authorized by the CCPA nor justified by the ISOR, nor would they help serve consumers. Rather, they are *ultra vires* rules that would lead to consumer confusion and frustration due to excessive, annoying pop-up notices all saying the same thing yet deterring users from quickly accessing the online and other content that they are most interested in viewing. Thus, CCTA recommends that these proposed regulations be deleted. In the alternative, the AG could replace these two provisions with a single simple regulation that faithfully implements the statutory mandate under 1798.185(a)(6), such as the

[37] *See* https://www.confidently.com/ and https://act.confidently.com/delete-digital-footprint.

[38] Government Code Sections 11346.2(b)(1) and 11346.3(a); and Section 1798.185(a)(1), (2), and (7).

[39] NOPA at 11.

[40] ISOR at 42 to 43.

[41] *See*, for example, pre-rulemaking comments filed with the AG by Interactive Advertising Bureau (at 464), Entertainment Association (at 745), and CCTA (at 503) among the compiled comments at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf.

following:

> 999.305 All of the notices and information that businesses are required to provide pursuant to the California Consumer Privacy Act shall be provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer.

F. Verification - Degree of Certainty: Proposed regulation 999.325 needs revision to provide clarity and be consistent with the CCPA framework that includes both regulations and separate agency guidance.

Article 4 of the proposed regulations includes "General Rules for Verification" (999.323), and additional rules for requests from consumers with password-protected accounts (999.324), non-account holders (999.325), and authorized agents (999.326). For non-account holders, proposed regulation 999.325 includes in subdivision (a) a requirement to comply with the general verification rules in 999.323. It also requires a business to comply with subdivisions (b) through (e), which the ISOR describes as providing "guidance" and illustrative examples of options for verification.[42]

Proposed regulation 999.325 provides as follows:

> "§ 999.325. Verification for Non-Accountholders
> (a) If a consumer does not have or cannot access a password-protected account with the business, the business shall comply with subsections (b) through (g) of this section, in addition to section 999.323.
>
> (b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a **reasonable degree of certainty.** A **reasonable degree of certainty** may include matching at least two data points provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer.
>
> (c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a **reasonably high degree of certainty**, which is a higher bar for verification. **A reasonably high degree of certainty** may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.
>
> (d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a **reasonable degree or a reasonably high degree of**

[42] ISOR at 31.

> **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**. A business shall 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.
>
> (e) Illustrative scenarios follow:
> (1) If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if the business maintains the consumer's name and credit card number, the business may require the consumer to provide the credit card's security code and identifying a recent purchase made with the credit card to verify their identity to **reasonable degree of certainty**.
>
> (2) If a business maintains personal information in a manner that is not associated with a named actual person, 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. This may require the business to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3).
>
> (f) If there is no reasonable method by which a business can verify the identity of the consumer to **the degree of certainty required by this section**, the business shall state so in response to any request and, if this is the case for all consumers whose personal information the business holds, in the business's privacy policy. The business shall also explain why it has no reasonable method by which it can verify the identity of the requestor. The business shall evaluate on a yearly basis whether such a method can be established and shall document its evaluation." (emphasis added)

CCTA objects to subdivisions (b) through (e) for several reasons. First, the provisions adopt a complex new construct to measure the "degree of certainty" applicable to different consumer requests. The provisions require verification to either a "reasonable degree of certainty" or a "reasonably high degree of certainty" with permissible options for achieving the applicable degree of certainty. This "degree of certainty" requirement is not based in the text of the CCPA and is not necessary to effectuate the purpose of that statute. The general verification requirements in proposed Article 4, combined with the clear statutory prohibition against a business acting on a consumer request unless verified, are sufficient to further the purposes of the CCPA.

Second, rather than advance clarity, the "degree of certainty" construct is highly subjective and would require businesses to add a complex and confusing new layer to the verification protocols they are currently implementing. The proposed regulation identifies factual scenarios that "may" require a specified degree of certainty, and then lists possible options that "may" meet that degree of certainty. Rather than a safe-harbor approach, the proposed regulation does not even specify a method of verification that will ensure compliance.

As the ISOR states, subdivisions (b) through (e) are primarily aimed at providing guidance. The illustrative examples could become quickly obsolete and may not be instructive by the time regulations are finalized. However, if adopted as regulations, these provisions will have the force of law, and thereby create confusion with compliance and enforcement until modified by another lengthy rulemaking process.[43] Significantly, the CCPA provides for the AG to provide "guidance on how to comply with the provisions of [the CCPA]" separate from formal regulations.[44] It would be more consistent with the statute and the framework the Legislature established to provide the fact-specific guidance intended by subdivisions (b) through (e) in a different format such as non-binding guidance memos or workshops.

Accordingly, CCTA recommends revising proposed regulation 999.325 as follows:

(a) If a consumer does not have or cannot access a password-protected account with the business, the business shall, in good faith, seek to verify any request in compliance ~~comply~~ with ~~subsections (b) through (g) of this section, in addition to~~ section 999.323.

(b) The Attorney General shall periodically issue non-binding guidance and best practice examples of verification procedures and processes that businesses may use to handle, assess, attempt to verify, and respond to requests from consumers with password-protected accounts (999.324), non-account holders (999.325), and authorized agents (999.326).

~~A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer.~~

~~(c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.~~

~~(d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. 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. A business shall 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.~~

~~(e) Illustrative scenarios follow:~~

~~(1) If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide~~

[43] Government Code Section 811.6 (state regulation adopted under APA has the "force of law.")

[44] Section 1798.155(a).

> ~~evidence that matches the personal information maintained by the business. For example, if the business maintains the consumer's name and credit card number, the business may require the consumer to provide the credit card's security code and identifying a recent purchase made with the credit card to verify their identity to reasonable degree of certainty.~~
> ~~(2) If a business maintains personal information in a manner that is not associated with a named actual person, 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. This may require the business to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3).~~
> ~~(f) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and, if this is the case for all consumers whose personal information the business holds, in the business's privacy policy. The business shall also explain why it has no reasonable method by which it can verify the identity of the requestor. The business shall evaluate on a yearly basis whether such a method can be established and shall document its evaluation.~~

G. **Recording Keeping Requirements: Proposed regulation 999.317 needs revision to ensure clarity for compliance and to be consistent with the CCPA authorizing consumers to make requests through a variety of technologies.**

Proposed regulation 999.317 specifies training and record-keeping requirements for the stated purpose of specifying "the type of information businesses must retain to demonstrate compliance with the CCPA" and "to aid in enforcement of the law."[45] CCTA supports the flexibility provided in subdivision (c) of proposed regulation 999.317, which recognizes that businesses will utilize a variety of formats and methods for accepting consumer requests. However, CCTA recommends a revision to subdivision (b) of proposed regulation 999.317 so that the proposed regulation also recognizes how certain types of consumer requests may be submitted through a variety of technologies, which directly impacts the availability of records. For example, a consumer may submit a request to opt out of sale directly to the business or through privacy choices offered by whatever browser the consumer is using. In the case of social media plug-ins or third-party analytics cookies, consumers register their opt-outs directly with those entities. In those instances, the business would have no record of the consumer's request to opt out because the places where the opt-outs are maintained would not be within the control of the business.

Clarity on this point is necessary because the proposed regulation imposes a mandate that is not in the text of the CCPA,[46] and the mandate cannot be inconsistent with the statute.[47] Thus, CCTA requests that proposed regulation 999.317 be revised as follows:

> "§ 999.317. Training; Record-Keeping
> (a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all the requirements in the CCPA and these regulations and how to direct consumers to exercise

[45] ISOR at 26 to 28.
[46] ISOR at 26 (the CCPA is "silent on any specific training or record-keeping requirements").
[47] Government Code Section 11342.2.

their rights under the CCPA and these regulations.

(b) A business shall maintain, for at least 24 months, records of (i) consumer requests made pursuant to the CCPA through an operation within the control of the business, and (ii) how the business responded to ~~said~~those requests~~ for at least 24 months~~.

(c) The records may be maintained in a ticket or log format provided that the ticket or log 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.

(d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

(e) Information maintained for record-keeping purposes shall not be used for any other purpose.

(f) 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.

(g) A business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall:
(1) Compile the following metrics for the previous calendar year regarding consumer requests made pursuant to the CCPA through an operation within the control of the business:
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.

(2) Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.

(3) 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."

H. **Opt-Out Request Methods: Proposed regulation 999.315(a) should be deleted because it is not required by and is inconsistent with the CCPA, is not necessary given that the CCPA directly addresses opt-out requests, and inaccurately designates "acceptable" methods that would create consumer confusion.**

Proposed regulation 999.315(a) requires a business to provide two or more designated methods for submitting a request to opt out of the sale of personal information, one of which must be a link on the business's website or mobile application titled "Do Not Sell My Personal Information" or "Do Not Sell My Info." The proposed regulation specifies other "acceptable methods" as follows:

> "999.315 (a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive web form 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. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and 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."

The ISOR concludes that this proposed regulation is necessary based on the following rationale:

> "**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."[48]

With this statement, the AG acknowledges that the CCPA does not require a business to provide two or more methods for submitting opt-out requests, "as they are required to do for requests to know and request to delete." As set forth below, Section 1798.130(a)(1) is very clear and precise in referencing the other CCPA code sections when requiring "two or more methods for submitting requests":

> 1798.130 (a) In order to comply with Sections ***1798.100, 1798.105, 1798.110, 1798.115, and 1798.125***, a business shall, in a form that is reasonably accessible to consumers:
> (1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections ***1798.110 and 1798.115***, including, at a

[48] ISOR at 23 to 24 (emphasis added).

> minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.[49]

Significantly, Section 1798.120 – the CCPA's right to opt out of sale – is ***not*** included in the statutory text quoted above, reflecting clear legislative intent that this statutory mandate of two methods for submitting requests does not apply to requests to opt out. If the Legislature had wanted to make the mandate applicable to requests to opt out, it would have cross-referenced Section 1798.120 in Section 1798.130(a)(1). It is therefore inconsistent with the statute and beyond the scope of AG authority to impose that mandate through regulation.

Instead of including opt-out requests in Section 1798.130, the Legislature specified in Section 1798.135 a different set of requirements applicable solely to opt-out requests. These statutory requirements include that a business provide a "Do Not Sell My Personal Information" link on its website and in its privacy policy if the business has a privacy policy, but there is no requirement for at least two "acceptable" methods of submitting requests to opt out.

Nonetheless, the AG seems to be second-guessing the Legislature and assuming that the Legislature must have intended to also apply the two-method mandate to requests to opt out. The ISOR states that including this requirement in AG regulations is "necessary" to implement Section 1798.135 based on the assertion that the section does not address "business situations" not involving an online presence. However, multiple provisions in Section 1798.135 apply to any business, not just those with an online presence, including, for example, the requirement to include a description of consumers' opt-out rights in "a form reasonably accessible to consumers" in "[a]ny California-specific description of consumers' privacy rights,"[50] and a requirement that "all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all [statutory opt-out requirements] and how to direct consumers to exercise their rights."[51] This more general approach to ensure consumers have direction on how to exercise opt-out rights is both intentional and appropriate given that consumers will have many options for exercising opt-out rights – including options that are not necessarily within the control of a business, as discussed in Section II.B.

The proposed regulation, on the other hand, mandates at least two opt-out request submission methods that are pre-determined to be "acceptable." This is not consistent with the CCPA, nor is it necessary to effectuate the purpose of the statute. Instead, the proposed regulation would undermine the statutory purpose of enabling consumers to exercise their CCPA rights. For example, the proposed regulation states that a toll-free number to the business would be an "acceptable method." But if a consumer calls asking to opt out of all online sales, there would be no way for a customer service representative to implement that request because it must be done by the consumer himself at the relevant web page using the relevant opt-out mechanism(s), about which the customer service representative would have no knowledge and over which it would have no control. The result will be consumer confusion and frustration.

Thus, CCTA recommends that proposed regulation 999.315 be revised to delete subdivision (a).

[49] (emphasis added). Section 1798.110 refers to the right to know, and Section 1798.115 refers to the right to delete.
[50] Section 1798.135(a)(1).
[51] Section 1798.135(a)(3).

~~"999.315 (a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive web form 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. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and 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."~~

I. Categories of Third Parties: Proposed regulation 999.301(e) needs revision or should be deleted because it is factually inaccurate, inconsistent with the CCPA definition of "third party," and is not necessary given the existing statutory definition.

Although the CCPA already defines "third party," proposed regulation 999.301(e) defines "categories of third parties" in a manner that contradicts the statutory definition of "third party" and contains several significant factual inaccuracies. Proposed regulation 999.301(e) provides as follows:

> (e) "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.

On the other hand, the CCPA defines "third party" in Section 1798.140(w), which provides as follows:

> (w) "Third party" means a person who is not any of the following:
> (1) The business that collects personal information from consumers under this title.
> (2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:
> (i) Prohibits the person receiving the personal information from:
> (I) Selling the personal information.
> (II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
> (III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.
> (ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.
> (B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal

information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

The AG's proposed definition of "categories of third parties" is not consistent with this statutory definition of "third party" in that the proposed regulation states that third parties "do not collect personal information directly from consumers" and then identifies a non-exhaustive list of examples of third parties, including "internet service providers" ("ISPs"). CCTA member companies are ISPs, and they *do* have direct relationships with consumers and *do* collect personal information from them (e.g., to set up a broadband account), which makes it factually inaccurate to include ISPs in the proposed definition. The ISOR states that the proposed definition "identifies key categories of third parties, while at the same time leaving the list open-ended to allow for differing business practices."[52] However, as drafted, it makes "not collect[ing] personal information directly from consumers" a required element of the definition, which is inaccurate at least for ISPs, although the same would also appear to be true for "government entities" and "social networks," which also collect personal information directly from consumers. Moreover, in some cases, cable operators may function as "service providers" to businesses and thus, under the CCPA definition set forth above, would *not* constitute third parties, again making the proposed regulation both contrary to the CCPA and factually inaccurate.

Thus, CCTA recommends that subdivision (e) be deleted from proposed regulation 999.301 because it is factually inaccurate, inconsistent with the CCPA, and not necessary because the CCPA already has a sufficient definition of third party. At the very least, ISPs should be removed from the definition of "categories of third parties," although again that would not be a sufficient solution for this issue in CCTA's view because other entities listed in this definition also collect personal information from consumers.

> ~~(e) "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.~~

III. The AG should adopt CCTA's recommended revisions to the proposed regulations to help address the ISOR's serious failures to meet critical APA requirements and to accurately account for the cost of CCPA statutory and regulatory compliance.

A. The ISOR fails to fully describe the purpose, rationale, and material relied upon for each aspect of all proposed regulations and fails to account for the full cost of burden on business.

CCTA appreciates the AG's immense effort to draft regulations meant to implement the CCPA by the statutory deadline. It cannot be overstated that the CCPA is highly complex with wide-ranging impacts on consumers, businesses, and the overall economy. Since the CCPA was enacted on June 28, 2018, businesses have faced enormous challenges seeking to develop and implement processes to timely comply with the numerous CCPA requirements, many of which become operative in less than a month on January 1, 2020. Despite good faith and diligent efforts

[52] ISOR at 4.

by businesses, compliance challenges have been compounded by multiple moves of the legislative and regulatory goal posts – both in time and substance. For example:

- In June 2018, the CCPA was enacted to become operative on January 1, 2020.

- In October 2018, amendments to the CCPA were enacted to, among other changes, specify that enforcement of the CCPA would begin six months after final regulations are adopted by the Attorney General or July 1, 2020, whichever is sooner.

- By February 2019, more than a dozen bills proposing multiple substantive changes to the CCPA were introduced and considered by the Legislature throughout the 2019 legislative session, including proposals to change the operative date.

- In October 2019, AB 1355 (Chau) and AB 25 (Chau) were enacted, making some changes to the CCPA effective January 1, 2020, and excluding employees as consumers but only until January 1, 2021. Numerous other changes to the CCPA were under consideration until the final stage of the legislative session.

- In October 2019, the AG released proposed regulations that include many new requirements in addition to those already in current law.

- The AG is currently holding hearings on its proposed regulations, and given various internal reviews and processes required under California law, the final regulations are not likely to be published until well into next year, leaving businesses little time to review them or to adjust their operations to comply by the July 1, 2020 deadline.

- In November 2019, a new ballot initiative that would make significant changes to the CCPA and establish an entirely new agency for enforcement was filed with the AG. This new initiative would move the operative date to January 1, 2023 for most provisions (although earlier for some) and require enforcement of AG regulations – which dramatically swelled in the ballot initiative from seven areas of required regulations under the CCPA to an incredible 22 areas (some with multiple subparts) no later than July 1, 2023. Despite this new ballot initiative with all its significant new provisions, the CCPA and associated regulations remain on a shorter enforcement time period of January 1, 2020, and July 1, 2020, *even though various aspects of the CCPA and its regulations would be changed by the ballot initiative*.

In light of this history and the pending ballot initiative, CCTA is concerned that the ISOR does not adequately explain the rationale and justification for all of the AG's proposed regulations. The APA requires that an agency's ISOR provide a very detailed rationale for *each* proposed regulation and specifically identify the reports, documents, or other facts relied upon to justify the proposal. Full public disclosure of these details is necessary for transparency of the rulemaking process and for parties to be able to provide meaningful comments on all aspects of proposed regulations. Government Code Section 13346.2 subdivision (b) provides, in pertinent part, as follows:

> (b) An ***initial statement of reasons*** for proposing the adoption, amendment, or repeal of a regulation. This statement of reasons ***shall include***, but not be limited to, all of the following:
> (1) A statement of the ***specific purpose*** of each adoption, amendment, or repeal, the problem the agency intends to address, and the rationale for the determination by the agency that each adoption, amendment, or repeal is reasonably necessary to carry out the purpose and address the problem for which it is proposed….
> *
>
> (3) ***An identification of each technical, theoretical, and empirical study, report, or similar document, if any, upon which the agency relies in proposing the adoption, amendment, or repeal of a regulation***.
> (4) (A) ***A description of reasonable alternatives to the regulation and the agency's reasons for rejecting those alternatives***. Reasonable alternatives to be considered include, but are not limited to, alternatives that are proposed as less burdensome and equally effective in achieving the purposes of the regulation in a manner that ensures full compliance with the authorizing statute or other law being implemented or made specific by the proposed regulation….
> *
>
> (5) (A) **Facts, evidence, documents, testimony, or other evidence on which the agency relies to support an initial determination that the action will not have a significant adverse economic impact on business….** (emphasis added)

The ISOR does not meet these APA requirements in several respects. First, throughout the ISOR the AG states that proposed regulations are to address concerns raised in the pre-rulemaking activities.[53] But the ISOR does not cite to any specific comments filed in March 2019 or any statement made at the public hearings in January and February 2019 -- or even name any specific stakeholder who raised the concerns relied upon. It is unclear if concerns were raised by a single party or numerous stakeholders, or the level of credibility and expertise of the party who raised concerns. Not identifying the source and actual content of the concerns the AG claims to rely upon fails to meet the letter and spirit of Government Code Section 11346.2(b)(3) and (5). This approach also lacks transparency, which is the foundation of the public notice requirements in the APA. Moreover, as a practical matter, the ISOR citing only to concerns generally precludes other stakeholders from being able to analyze the specific basis for a proposed regulation and provide meaningful feedback in the 45-day comment period. With such a highly complex and technology-driven law as the CCPA, a transparent and open review of the complete rationale and factual basis for proposed regulations is critical to achieving the CCPA's statutory purpose.

Second, the AG's approach in the ISOR of citing only to general public concerns raised in pre-rulemaking activities makes it nearly impossible to assess compliance with the requirement in Government Code Section 11346.2(b)(4) to provide a "description of reasonable alternatives" to a proposed regulation and the agency rationale for preferring one alternative over others. For example, regarding proposed regulations 999.305 and 999.308, the ISOR states that these duplicative and lengthy notice requirements address concerns raised in pre-rulemaking activities. But the record from the January and February public hearings and March comments contain numerous concerns regarding consumer notice from a wide range of parties who offer a variety of

[53] *See*, for example, ISOR at 10, 17, 26 and 28.

alternatives for achieving that notice. CCTA's comments, for example, urged a single notice as the best alternative for consumers to understand their rights.[54] Without a listing of all alternatives proposed in the record and identifying the source, it cannot be determined if all alternatives were considered and the reason for accepting or rejecting them as required by the APA. In addition, review of the full record is required to determine if "substantial evidence" exists to support regulations adopted under the APA. An agency cannot selectively cite to only the portion of an administrative record that supports its proposed regulation and ignore the rest.[55]

Third, the rationale provided in the ISOR for each proposed regulation may provide a general reason but does not articulate the "specific" detail required by the APA. As explained in comments above regarding individual proposed regulations, many are multi-faceted with various requirements and new mandates not based in express terms of the statute. In many cases, the ISOR lacks detail regarding the purpose of the proposal and the operational changes needed to implement it. For many proposed regulations, the ISOR makes only a general reference to the burden on business and obstacles to implementation, thereby failing to meet the express direction of the Legislature in the APA and CCPA.[56]

Businesses, including cable operators, are already very far along – at enormous personnel allocation, dedication, and expense – with implementing protocols and operations to comply with the CCPA's January 1, 2020, operative date.[57] Businesses could not afford to wait to make choices and investments until AG regulations were finalized, and have been forced to choose compliance alternatives and proceed with implementation plans. The integration of privacy protocols across a wide scope of business operations makes it extremely costly, unreasonable, and in some cases technologically infeasible to shift course once again upon publication of final regulations, which in all likelihood will not occur until very close to the July 1, 2020 enforcement date. And no sooner than when these regulations are finalized and businesses are scurrying to review them and earnestly adjust their recently launched CCPA compliance operations to try and comply with them will the new ballot initiative significantly move the goal posts once again.

B. **The ISOR cost impact analysis fails to accurately account for the significant costs of proposed regulations that exceed the scope of the CCPA and the cost of multiple changes to requirements.**

The Standardized Regulatory Impact Assessment ("SRIA"), which is Appendix A to the ISOR, concludes that the cost to California businesses of complying with the CCPA could be $55 billion over the next 10 years, with up to $16 billion of that total due to the proposed AG regulations and the remainder a result of the underlying statute even without any regulations.[58] At the same time, the SRIA points to a lack of "empirical evidence to support a compliance cost

[54] CCTA comments filed with the AG on March 8, 2019 (at 503).

[55] Government Code Section 11349(a) ("Necessity" of a regulation "means the record of the rulemaking proceeding demonstrates by substantial evidence the need for a regulation to effectuate the purpose of the statute, court decision, or other provision of law that the regulation implements, interprets, or makes specific*, taking into account the totality of the record*") (emphasis added).

[56] Section 1798.185(a)(1), (2), and (7), and Government Code Sections 11346.2(b)(1) and 11346.3(a).

[57] SRIA at 9 (describing "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").

[58] SRIA at 8 and 11.

estimate,"[59] concludes that "the direct CCPA compliance costs are subject to considerable uncertainty,"[60] and issues the following caution:

> "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."[61]

CCTA is very concerned that $16 billion is an enormous incremental cost for California businesses to have to bear for compliance with the new regulations, but equally importantly that the SRIA reflects some fundamental misunderstandings of the cost of CCPA statutory and regulatory compliance and associated burdens on business. First, the SRIA concludes that business "operational costs" and "technology costs" are almost entirely attributable to the CCPA and that businesses will incur these costs even before the regulations are drafted.[62] The SRIA points to "ongoing training requirements and some record-keeping requirements," along with "some design costs" for web pages as the universe of incremental costs resulting from the AG's proposed regulations.[63] This assessment simply fails to account for how the proposed regulations impose new mandates that exceed the scope of the CCPA. Incredibly, the SRIA inaccurately concludes that the proposed AG regulations relating to customer notice will result in *no* new costs to business.[64] As explained in Section II.E., the proposed regulations require duplicate notice and with more detail well beyond what is required in the text of the CCPA. This one regulation alone will impose substantial additional costs to create the new notice in a legally compliant manner, create new mechanisms for displaying it to consumers wherever personal information is collected, train customer service representatives to field questions about the notice, monitor ongoing compliance, etc.

Second, the SRIA incorrectly assumes that operations and technology compliance costs are one-time:

> "Operational costs are predominantly a one-time cost of establishing workflows, plans, and other inter-departmental non-technical systems to determine the business's best compliance pathway under the CCPA. These costs are largely labor costs associated with meetings and compliance planning."[65]

Again, this assessment fails to reflect the significant costs that businesses have had to incur, and will continue to experience going forward, to continuously adjust their compliance plans and operations with the constant changing of the goal posts for CCPA compliance as set forth in the brief history listed above. If the proposed regulations were adopted as is without any changes, many protocols and practices already implemented by many thousands of businesses to meet the January 1, 2020 effective date will need to be changed once again. The SRIA significantly

[59] SRIA at 29.
[60] SRIA at 36.
[61] SRIA at 29. The Department of Finance letter attached to the SRIA states very general concurrence with the methodology used to estimate cost impacts of the proposed regulations but is silent as to any assessment of how the proposed regulations exceed CCPA statutory requirements. The letter is dated September 16, 2019, a month prior to the AG releasing the proposed regulations.
[62] SRIA at 10 to 11, and 16 to 19.
[63] SRIA at 11.
[64] SRIA at 19.
[65] SRIA at 24.

understates the actual, real-world impact of the current proposed regulations on businesses – and does not even anticipate or try to account for the enormous new costs that would be imposed on businesses were the new ballot initiative to be adopted, including its 22 new sets of (often multi-part) rules (as opposed to only seven in the CCPA).

CCTA therefore respectfully urges the AG to take into account the foregoing serious APA shortcomings and the dramatic cost increases that will be imposed on businesses by the new regulations – well beyond what the CCPA would require and well short of what the new ballot initiative would mandate if approved by the voters. CCTA recommends that the AG, at the very least, accept the revisions to the proposed regulations recommended herein by CCTA, which are designed to address and help mitigate these substantial APA and cost issues in reasonable ways that will not reduce consumer privacy protections. Only in so doing could the AG say it has endeavored to consider the genuine obstacles and burdens its proposed regulations would otherwise have on businesses, and also reasonably balanced and minimized those obstacles and burdens even as it seeks to enhance consumer privacy.

IV. Conclusion

CCTA respectfully requests that the AG accept the revisions to the proposed regulations recommended in these comments in order to comply with clear direction in the APA and CCPA to adopt reasonable regulations that advance consumer privacy while minimizing implementation obstacles and burdens on business.

Respectfully submitted,

/s/Jacqueline R. Kinney

Jacqueline R. Kinney
CCTA Senior Vice President and General Counsel

Message

From: Kyla Christoffersen Powell [redacted]
Sent: 12/7/2019 12:58:02 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CJAC Comments on CCPA Regulations
Attachments: CJAC Comments CCPA Regulations 12-6-19.pdf

Dear Privacy Regulations Coordinator:

Attached are CJAC's comments on the CCPA Regulations.

Best regards,

Kyla Christoffersen Powell
President and Chief Executive Officer
[redacted] www.cjac.org
CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

December 6, 2019

Xavier Becerra, Attorney General
California Department of Justice
1300 I Street, Suite 1740
Sacramento, CA 95814

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

Re: *Comments by the Civil Justice Association of California on Proposed Regulations for the California Consumer Privacy Act*

Dear Attorney General Becerra:

The Civil Justice Association of California ("CJAC") is a more than 40-year-old nonprofit organization representing a broad and diverse array of businesses and professional associations. A trusted source of expertise in legal reform and advocacy, we confront legislation, laws, and regulations that create unfair burdens on California businesses, employees, and communities. Toward that end, CJAC offers research and guidance on policy issues that impact civil liability issues, including the following comments on the Attorney General's proposed regulations (§§ 999.313(c)-(d), 999.323) defining the scope and application of the California Consumer Privacy Act (CCPA).

Many businesses attempting to comply with the CCPA find it complex and vague, making implementation difficult. The regulations can serve to provide needed clarifications and guidance to businesses. CJAC appreciates the significant work of the Office of the Attorney General to date in developing the proposed regulations and the clarifications they do provide. For example, the balancing tests laid out for responding to personal information requests - weighing the benefit to the consumer versus security risks - is a helpful clarification. (§§999.313(c).), 999.323.) Additionally, providing guidance on acceptable forms of deletion, such as deidentification, also provides guidance that strikes a proper balance between consumers' rights and business and public benefit. (§999.313(d).)

As spelled out below, however, CJAC has some concerns, that some areas of the regulations do not provide necessary clarifications, are too burdensome, or have significant gaps.

Regulations needing revision due to lack of clarity or undue burden:

- **§ 999.313(b) Responding to Requests to Know and Requests to Delete.** This proposed regulation states that the 45-day deadline to respond begins to run on the day the business "receives a request, regardless of time required to verify the request." This deviates from the CCPA which states that a business must disclose and deliver required information to a consumer within 45 days upon "receiving a *verifiable* request." (Civil Code § 1798.130)(a)(2)(emphasis supplied).) Rather than making the 45-day deadline more stringent than the statute, the regulations should provide guidance on what is a reasonably verifiable request, as directed by the CCPA under Civil Code §1798.140(y): ""Verifiable consumer request" means a request made by a consumer ... that the business can reasonably verify, pursuant to regulations adopted by the Attorney General." Accordingly, the 45 days should only begin to run if the consumer request is reasonably verifiable. Indeed, under the same section, a business has no obligation at all to provide the information if the business cannot verify the consumer. (Civil Code § 1798.140(y).)

Alternatively, this regulation should clarify that the "necessity" required to "take up to an additional 45 days" [beyond the first 45 days to respond to a consumer's request to know or delete information] is satisfied if the business has been unable to "verify" the consumer's identity. The regulation recognizes businesses' responsibility to verify requests properly, a task that may take days or weeks to complete and is reliant upon a consumer's cooperation in providing accurate information in a timely manner. After a request is "verified," a company must then find the information it holds on a consumer – information which may be kept in separate databases – and convert it into a form which can be delivered to the consumer. Since "receipt of the request" itself initiates the initial 45-day period, businesses seeking to comply and avoid liability are spurred to ascertain that the request is made by the consumer and not an imposter. Specifying that a business is entitled to the 45-day extension if the consumer's identity cannot be verified within the first 45-day period furthers the public interest.

- **§ 999.313(d)(1) Responding to Requests to Delete**. Consumer requests to delete personal information that cannot be verified should not be treated as "opt-out" requests. Businesses should act upon requests when a consumer expresses a clear preference, but regulations should not presuppose a consumer's choice by treating an unverified delete request as a "do not sell" preference. Additionally, this presupposition could result in businesses having to opt out all non-Californians who make a deletion request, if they are unable to verify the consumer's California residency status. The CCPA provides consumers with several distinguishable rights to exercise. Requiring businesses to conflate these requests reduces real consumer choice inconsistent with the CCPA.

- **§ 999.315(c) & (g) Requests to Opt-Out**. CJAC has serious concerns and doubts about the viability of the requirement that businesses treat browser plug-ins or settings as "opt-out" requests under the CCPA. These technologies were designed for and in other contexts that are not compatible with the CCPA's complex and extremely broad definitions of "sale" and "personal information."

  The CCPA emphasizes consumer choice and defines a mechanism – the "Do Not Sell" button – that businesses must make available on their Web sites so consumers can exercise choices. It is not consistent with the statute to create this additional mechanism, nor is it clear that consumers, who use plug-ins, intend to use them to opt out of CCPA sales.

  Browser-based opt-out technology is not now sufficiently interoperable and developed to ensure that all parties that receive such a signal can make it operable. Accordingly, CJAC instead supports industry-based efforts for more than a year to develop consistent technical signals for "Do Not Sell" technology.

- **§ 999.325 (c) Verification for Non-Accountholders**. This regulation should be revised to clarify that a business's execution and maintenance of" a signed declaration under penalty of perjury" to verify consumer requests is optional. The regulation indicates this is an option among others by stating that "a reasonably high degree of certainty *may* include ... a signed declaration under penalty of perjury" (emphasis supplied). An optional approach is appropriate, as a blanket requirement would be burdensome and unnecessary given the technological ability to obtain "verification."

- **§ 999.314 (c) Service Providers**. This regulation restricts service providers beyond the intent of the CCPA, which allows a business, under certain circumstances, to use or share personal information with a service provider that is necessary for a legitimate business purpose. The proposed regulation, however, limits what businesses and service providers may do with data in a way that is unnecessary and threatens to harm the data economy. For example, given the broad definition of "personal information," this provision restricts a business's ability to use its data for legitimate business purposes agreed to by contract where personal information will not be sold but only used by the service provider to provide services to the business. This proposed regulation goes beyond the standards defined by the CCPA.

- **§999.316(a) Requests to Opt-In to the Sale of Personal Information.** Requiring a two-step opt-in process as this provision would do is unnecessary and creates consumer confusion. This requirement is neither consistent with other laws nor consumer expectations. It requires businesses to build new systems that make users jump through unnecessary hurdles to express a preference. It nudges consumers toward a course of action rather than empowering them to make their own decisions in a straightforward manner.

  It is also inconsistent with the regulation allowing businesses to use personal information for additional purposes beyond those previously disclosed to the consumer with explicit consent rather than a two-step opt-in process. (§999.305(a)(3)). The CCPA expressly adopts an "opt-out" regime rather than one that is "opt-in", making this proposal inconsistent with the statute. (*See*, §§1798.115, 1798.120.) Further, data protection principles typically do not require additional consent for use of data that is consistent with the context in which the consumer receives the service.

- **§ 999.317 Training; Record-Keeping**. The reporting requirements exceed the scope of the CCPA and are not related to its purposes. Nowhere in the CCPA is there a provision regarding record-keeping, and it is unclear what policy goal this requirement seeks to fulfill. It imposes a burden on businesses which does not appear tied to consumer benefits or rights and requires the collection of additional personal information beyond the scope of the CCPA.

  Imposing additional record-keeping and disclosure requirements on businesses that handle the personal information of 4 million or more consumers is unwarranted. The CCPA requires businesses to provide multiple disclosures to consumers, and this regulation's requirement for more information does not provide them with a greater understanding of their privacy protections.

- **§ 999.307(b)(5) Notice of Financial Incentive**. This regulation requiring disclosures about financial incentives is impractical and threatens confidential, competitively sensitive information. It is challenging for any business to assign value to a single consumer's data, and data often gains value when it is aggregated. Consequently, financial incentive programs will more likely be based on a complex calculation of costs to the business and market comparisons that is unlikely to be meaningful to consumers.

  There are significant differences between businesses and the services they provide. Requiring all businesses to disclose its methods and calculations will likely require disclosure of competitively sensitive information. The CCPA is sufficiently protective of consumers with regard to discounts; and this regulation unnecessarily goes beyond that protection.

- **§ 999.305(d)(2) Notice at Collection of Personal Information**. Greater flexibility respecting notice before resale of data is needed. Regulations should clarify that a business receiving personal information from an indirect source may comply with CCPA obligations by written agreement requiring other businesses to provide the requisite notice to consumers. Requirements to contact the "source" and obtain "signed attestations" are burdensome and unnecessary.

- **§ 999.301(e) "Categories of third parties"**. The definition of "categories of third parties" is overly broad. Internet service providers (ISPs) and social networks, for example, generally have a direct relationship with consumers. Although some may receive personal information indirectly at times, ISPs and social networks that do not do so should be removed from the third-party definition.

Regulations that are missing:

- **Regulations should specify that enforcement will be delayed until January 1, 2022.** Since the CCPA does not dictate an effective date for regulations, the Attorney General has discretion to establish an effective date for enforcement purposes. The CCPA merely states the Attorney General should "adopt regulations" by July 1, 2020 and provides that the *earliest* date that such enforcement could be brought is "six months after the publication of the final regulations ... or July 1, 2020, whichever is sooner" (emphasis supplied). Given the complexity of the CCPA and the proposed regulations and substantial implementation and compliance burden on businesses, a delayed enforcement date is necessary and justified.

- **Regulations should clarify the jurisdictional scope of the CCPA**. The CCPA's broad definition of "business" suggests a sweep within its ambit of non-U.S. businesses that incidentally collect personal information about a single California resident. Regulations should clarify that a business whose operations are outside of California and who only collect a *de minimis* amount of personal information from California residents are not required to comply with CCPA. Alternatively, the regulations should provide that businesses operating outside California that do not target their services to California residents are not subject to the CCPA.

- **Regulations are needed to clarify the CCPA's "private right of action."** The CCPA specifies that recoverable "statutory damages" – *i.e.*, those "not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident" – may only be sought if a consumer first gives the defendant 30 days written notice of the violations and an opportunity to "cure" them.

"Cure" is not defined in the CCPA provision. While not the subject of the proposed regulations, the proposed privacy initiative for the November 3, 2020 ballot adds a sentence to this section (which does not take effect until January 1, 2023, three years after its enactment) stating that the "implementation and maintenance of reasonable security procedures and practices . . . following a breach does *not* constitute a cure with respect to that breach." So while we know what does *not* constitute a "cure" from the initiative, we don't know what qualifies as one under it or CCPA.

Does omission of this sentence in the CCPA mean that the "implementation and maintenance of reasonable security procedures and practices" by a business within the 30-day notice period *does* count as a "cure"? CJAC submits that it should. Additionally, the regulations do not provide guidance on what is "reasonable security," which is also not defined by the CCPA and ripe for litigation. These uncertainties can and should be clarified by regulation.

Gaps in needed clarification or regulations that are too burdensome will give rise to unnecessary and unproductive enforcement actions and litigation. The goal of the regulations should be to facilitate implementation of and compliance with the CCPA – a win-win for consumers and businesses.

Thank you for your consideration,

Kyla Christoffersen Powell
President and Chief Executive Officer

Message

From: aj@clta.org [redacted]
Sent: 12/5/2019 10:50:32 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Craig C. Page [redacted] John Caldwell [redacted]
Subject: CLTA Comments on Notice of Proposed Rulemaking Action Relating to the California Consumer Privacy Act
Attachments: CLTA Comments to AG RE CCPA 120519.pdf

December 5, 2019

To Whom It May Concern:

Please find attached an electronic copy of the California Land Title Association's Comments on the Department of Justice's Notice of Proposed Rulemaking Action relating to the California Consumer Privacy Act (§§ 999.300 – 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations, October 11, 2019). These comments are also being sent in a hardcopy format.

Thank you for your time and consideration.

Sincerest Regards,

Anthony Helton
Legislative Coordinator
California Land Title Association
1215 K Street, Suite 1816 | Sacramento, CA 95814
[redacted]

CLTA California Land Title Association

SINCE 1907

December 5, 2019

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

RE: CLTA Comments on Notice of Proposed Rulemaking Action (§§ 999.300 – 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations, October 11, 2019) ("Proposed Regulations")

To Whom It May Concern:

The California Land Title Association ("CLTA") appreciates the opportunity to provide comments on regulations proposed pursuant to the California Consumer Privacy Act ("CCPA") on behalf of its members for consideration by the Attorney General and his staff.

CLTA is a non-profit trade organization founded in 1907. Our members employ thousands of professionals throughout California dedicated to the efficient and competent closing of real property transactions and the issuance of title insurance in connection with such transactions.

Based in Sacramento, the Association effectively serves as a resource for both title insurers and underwritten title companies who serve consumers in all 58 counties providing research regarding and insuring the status of title to real property, as well as acting as the escrow and settlement agent in the sale and transfer of real property, refinancing of loans, and other related functions.

We appreciate the Attorney General's efforts to provide guidance regarding specific aspects of the CCPA via the Proposed Regulations. In response, we respectfully offer the following comments on elements of the Proposed Regulations in furtherance of the Attorney General's goals, thereby aiding business' efforts to comply with, and consumers' understanding of, the CCPA.

As currently drafted, the definition of "household" in the Proposed Regulations would create unnecessary ambiguities with respect to consumers' rights and business' obligations under the CCPA:

The definition of "personal information" within the CCPA extends beyond a single consumer's information by also including information tied to a "household," thereby enabling a consumer to make a verifiable request for personal information belonging not only to themselves but also other household members. Because the disclosure of a consumer's personal information to other persons would work counter to the aims of the CCPA, it is therefore critical that the Proposed Regulations clearly define the term "household" so as to protect consumers from an unintended disclosure of their personal information to passing acquaintances, roommates, and others they may not consider members of their "household."

Contrary to this goal, the current definition of "household" in the Proposed Regulations is unnecessarily broad and ambiguous and will leave open to interpretation whether or not the data of a temporary visitor or others is considered "household" data under the CCPA:

> Proposed Regulations Section 999.301(h):
>
> (h) "Household" means a person or group of people ***occupying*** a single dwelling. (Emphasis added)

While the term "household" is an undefined legal term within the CCPA, it was logically chosen by the Legislature to mean only people who actually live in a residence and share the same living space on more than a temporary basis. A "household" logically applies only to those people who ***live*** together at the same residence and, furthermore, in the context of personal information, share common access to devices or services.

Since the term "occupying" is not further defined in the Proposed Regulations as it relates to "household," the above definition of "household" as articulated in the Proposed Regulations could be interpreted to mean that ***any*** person or group of people who happen to ***occupy*** a single dwelling for ***any period of time*** (e.g. minutes, hours, or a couple of days) would be considered a member of the household for purposes of the regulations and the CCPA. Furthermore, consumers that reside together but do not share any common access to services or devices – such as roommates – would also fall under the definition in the Proposed Regulations. Thus, the definition of "household" as proposed would create a "floating target" that is difficult, if not impossible, to track.

Such a "floating target" will result in a number of unintended consequences:

- A stranger, friend, or family member who happened to share a dwelling space --*for any amount of time*— with another consumer would arguably have the ability to request the personal information of members of the real "household" members via a request to know.
- Under such a definition, businesses attempting to comply with the CCPA would not be able to rely upon a more common-sense approach, such as people who actually reside together and share access to a single device or service.

To eliminate this ambiguity, we respectfully propose the following amendments to the Proposed Regulations:

> Proposed Regulations Section 999.301(h):
>
> (h) "Household" means ~~a person or group of people~~**two or more consumers** occupying ~~a single dwelling~~**the same residential address as their primary residence and that share common access to a device or service provided by a business**.

As used within Notice at Collection, Notice of Right to Opt-Out, Notice of Financial Incentives, and Privacy Policy accessibility provisions, the term "disabilities" should be more clearly defined by referencing longstanding California law:

The Proposed Regulations require three separate Notices – Notice at Collection, Notice of Right to Opt-Out, and Notice of Financial Incentives – as well as a business's privacy policy, to "be accessible to consumers with disabilities." However, by neglecting to clearly define what constitutes a disability, the Proposed Regulations do not provide businesses with sufficient guidance in complying with the CCPA.

We therefore respectfully propose the following amendments to the following four subsections in order to more clearly define business's obligations with respect to making the aforementioned disclosures available to consumers with disabilities in accordance with existing California law:

> Proposed Regulations Sections 999.305(a)(2)(d), 999.306(a)(2)(d), 999.307(a)(2)(d), and 999.308(a)(2)(d):
>
> (d) Be accessible to consumers with **mental or physical** disabilities**, as those terms are defined in Government Code Section 12926**. At a minimum, provide information on how a consumer with a disability may access the policy in an alternative format.

Government Code Section 12926, enacted under the Fair Employment and Housing Act, provides a broader definition of disability than that afforded under the American Disabilities Act of 1990 and ensures that the definition remains consistent with California law. A pamphlet published by the California Department of Justice in 2003, titled "Legal Rights for Persons with Disabilities", states that Government Code Section 12926 defines mental or physical abilities as any "any mental or psychological disorder…" or "any physiological disease, disorder, condition…", respectively, "…that limits a major life activity." [1]

We believe this change will assist businesses in their efforts to comply with and operationalize under the CCPA by allowing them to adhere to longstanding practices with respect to providing nondiscriminatory access to information to disabled consumers as required by California law.

The definition of "typical consumer" within the Proposed Regulations is unnecessarily broad and incongruous with the definition of "consumer" under the CCPA:

The Proposed Regulations define "typical consumer" as "a natural person residing in the United States." Such a definition is much broader than, and incongruous with, the definition of "consumer" provided under the CCPA as found in Civil Code Section 1798.140(g):

> California Civil Code Section 1798.140(g):
>
> (g) "Consumer" means a natural person who is a ***California resident***, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.
> (Emphasis added)

We respectfully suggest the following amendment to the definition of "typical consumer" within the Proposed Regulations for the purpose of harmonizing the final rule with current California law as enacted via the CCPA:

> Proposed Regulations Section 999.301(s):
>
> (s) "Typical consumer" means a natural person residing in ~~**the United States**~~**California**.

By providing greater consistency in what the law considers to be a "consumer" or "typical consumer", we believe that the proposed change will provide clearer guidance in business' operational efforts to implement the CCPA.

As California has taken the important step of recognizing privacy as an individual right and providing consumers with meaningful privacy protections, it is critical that the Attorney General also consider the impacts of the CCPA on business and how the law's goals can be met while still enabling businesses to provide the vital products and services on which their customers rely.

CLTA supports the Attorney General's efforts to seek public comment on how to best implement regulations pursuant to the CCPA and appreciates being given the opportunity to respectfully suggest amendments. We believe that the aforementioned suggestions meaningfully further the Attorney General's goals in enacting the Proposed Regulations, thereby mitigating the risk of unintended negative consequences and improving the effectiveness of the CCPA.

Respectfully,

Craig C. Page
Executive Vice President
and Counsel

[1] Legal Rights for Persons with Disabilities [Pamphlet]. (2003) Sacramento, CA: California Department of Justice.

Message

From: Jarrell Cook [redacted]
Sent: 12/7/2019 12:49:49 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Lance Hastings [redacted]; Gino DiCaro [redacted]; Nicole Rice [redacted]
Subject: CMTA Comments on the CCPA Regulations
Attachments: CMTA -- Comments on CCPA Rules (2019).pdf

To Whom it May Concern:

Attached please find comments on the proposed regulations to implement the CCPA submitted on behalf of the California Manufacturers and Technology Association (CMTA).

Thank you for the opportunity to provide feedback.

Jarrell Cook

Partner | Resolute

[redacted]

1215 K St, #1100
Sacramento, CA

www.resolutecompany.com

CMTA
CALIFORNIA MANUFACTURERS
& TECHNOLOGY ASSOCIATION

December 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street, First Floor
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

Re: California Manufacturers and Technology Association Comments on the Proposed California Consumer Privacy Act Regulations

Dear Attorney General Becerra:

The California Manufacturers & Technology Association ("CMTA") appreciates the opportunity to comment on the proposed regulations regarding the California Consumer Privacy Act of 2018 ("CCPA").

CMTA represents 400 businesses from the entire manufacturing spectrum – including large, medium, and small manufacturers – generating more than $280 billion every year and employing more than 1.3 million Californians.

The aim of the CCPA is to enhance Californian's privacy rights and control over their personal information. As we noted in our March 8 Pre-Rulemaking Comments, a critical area for growth in the manufacturing industry is in the creation and use of connected devices – the network of physical objects embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data commonly described as 'The Internet of Things' ("IOT"). Connected devices made for and used by consumers will require thoughtful policy that balances privacy concerns with rules that still enable this emerging technology to function.

However, the implications of the CCPA and the proposed rules raise concerns for manufacturers using connected devices and collecting information for the purpose of production, not profiting from the sale of a customer's personal information. Manufacturers use connected devices in the industrial context to collect production data and gain valuable insights into the efficiency of their operations. Doing so reduces costs, improves safety, raises productivity, and increases their ability to effectively compete with their rivals across the world.

This sophisticated form of manufacturing is quickly becoming the industry standard. We are writing to draw your attention to concerns regarding the use of employee information that may frustrate manufacturers' use of this powerful technology in California. We also recommend adopting a minor clarification in the proposed regulation's provisions regarding household information.

I. Employee Information Generated from Manufacturers' Equipment and Facilities

Manufacturing employees generate a significant amount of information using IOT-enabled equipment that automates data collection. Manufacturers can improve their operations as they monitor data that reveals cost-saving assembly solutions, tracks inventory, monitors their products as they move through the supply chain, reduces safety hazards, and improves product quality. The future of manufacturing lies in the increasingly efficient use of data to manage operations and increase productivity.

The CCPA's broad definition of consumer includes employees and potentially provides them rights over certain information. This is poised to create confusion for California manufacturers if the proposed regulations do not create a clear line distinguishing the data an employee generates as a result of their relationship with the employer and their own personal information.

AB 25, by Assembly Member Ed Chau, recognized this potential confusion and created a one-year exemption for personal information that is collected from job applicants and employees from the rights the CCPA grants consumers. On January 1, 2021, that exemption will sunset and these proposed regulations will apply to employee generated data.

Manufacturers are concerned about operating their data-driven facilities under this unclear framework. Under the CCPA, a consumer – an employee – may opt out of the sale of their personal information. The CCPA's definition of sale is broad and covers any transfer or disclosure of the information to another business or third party for monetary or other valuable consideration. This could include manufacturer's use of operating systems and platform or other third-party services to analyze or capitalize on the production-related data their employees generate using their equipment.

Manufacturers are also prohibited, under the CCPA, from engaging in any discriminatory treatment for an employee's exercise of their right to opt-out of the sale of personal information. Manufacturers could still be obligated to provide an employee with the same financial incentive (e.g., a bonus for meeting a production quota, shift hours, etc.) or services and benefits. This provision would be unworkable if applied to data employees generate while using manufacturers' equipment. An employee that opted out of sharing the information their work generates with a third party that the manufacturer relies on for data management and analysis creates a blind spot in the manufacturers' production and supply chain. Employees opting out necessitates discriminatory treatment.

And the regulations do allow for such discriminatory treatment if it is "reasonably related to the value of the consumer's data as defined in section 999.337." In this context, manufacturers would be required to estimate the value of an individual employee's data generated using a manufacturers' equipment.

But treating employees as consumers in this context is unworkable and fundamentally flawed. This production and logistic data would not exist but for the manufacturer providing the employee with the tools and equipment necessary to generate the data. The data itself has no independent value outside of the manufacturers generation and use of the information. And it is difficult-to-impossible to parse out the marginal value of an employee's data at a specific phase of production.

Recommendation: Add language that clarifies that information generated using equipment, materials, and facilities owned by the employer and provided to an employee is not "personal information" for the purposes of the CCPA. This is a common-sense clarification that avoids confusion and comports with the public's general understanding of information use and ownership. Such language would not adversely impact consumers – under this scheme, employees would still retain any privacy rights to the personal information they own and generate independently of the employee relationship.

This clarification avoids unnecessary confusion that would otherwise prompt manufacturers to question whether they will face increased obligations and exposure to legal liability that will prevent them from locating their advanced production facilities in California.

II. Household Information

Manufacturers have some concerns regarding the definition of "household" in the proposed regulations. Connected devices, such as appliances or shared electronics, can generate data for any number of persons that are in a household. It is important for both the consumer and the manufacturer that the person or persons empowered to access and delete information about a household under the CCPA be clearly defined.

Section 999.301(h) defines household as a "person or group of people occupying a single dwelling."

Recommendation: Please clarify or, if necessary, amend the definition to be consistent with the general understanding that occupation requires continuous, non-transient possession of the property.

Please also revise Section 999.318(b) for clarity and consistency. The provision describes how a business may respond to requests to access or delete household information, granting rights to both "consumers of the household" and allowing for verification of all of the "members of the household."

Accordingly, Section 999.318(b) should be amended to read:

> "*If all consumers occupying 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 occupants of the household subject to verification requirements set forth in Article 4, then the business shall comply with the request.*"

We appreciate the work your office has done to address the workability issues raised in our March 8 letter. Many of the concerns regarding the interoperability of connected devices, household data, and responding and verifying consumer requests were satisfactorily addressed.

Due to the breadth of manufacturing industry, many sub-sectors – such as automobile manufacturers, machine and equipment makers, pharmaceutical producers, etc. – are also uniquely impacted by the CCPA. CMTA strongly supports their recommendations and requests for clarification on the proposed regulations.

Manufacturers also share the concerns that the CCPA raises for every business operating in California – they operate websites, market their products, notify consumers about recalls, and offer coupons and customer rewards. We encourage you to consider proposed changes that improve the CCPA's workability in these aspects as well.

Sincerely,

Jarrell Cook

Jarrell Cook
Consultant, Government Relations
California Manufacturers & Technology Association

Message

From: Alisa Reinhardt [redacted]
Sent: 12/7/2019 12:58:50 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CNCDA Comments re: CCPA Regulations
Attachments: CNCDA letter to AG re CCPA.pdf

Good afternoon,

Please find, attached, our Association's comment letter on the proposed CCPA regulations.

Thank you,

Alisa Reinhardt
Director of Regulatory Affairs
California New Car Dealers Association
1517 L Street
Sacramento, CA 95814
[redacted]

Serving California's Franchised New Car Dealers Since 1924

CNCDA

California New Car Dealers Association

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, California 90013

RE: California Consumer Privacy Act Proposed Regulations

Attorney General CCPA Regulations Team:

The California New Car Dealers Association (CNCDA) is a statewide trade association that represents the interests of 1,200 franchised new car and truck dealer members. CNCDA members are primarily engaged in the retail sale and lease of new and used motor vehicles, but also provide customers with parts, service, and automotive repair. CNCDA focuses primarily on (1) protecting and promoting the interests of franchised new car dealers before all state government and regulatory agencies and (2) providing compliance advice to best support our dealer members so that they can provide the best products and services to consumers and maintain high employment rates. We are providing comments and suggestions on these proposed regulations today on behalf of our dealer members.

California's new car dealers will endeavor to comply with all new requirements imposed on businesses pursuant to the California Consumer Privacy Act ("CCPA"). However, we think the proposed regulations should be modified to assist dealers in their compliance efforts.

Pursuant to California Government Code § 11349, adopted regulations must meet all the following standards:

(1) Necessity.
(2) Authority.
(3) Clarity.
(4) Consistency.
(5) Reference.
(6) Nonduplication.

In addition, one of the stated goals of Civil Code Section 1798.185(a)(7) is to minimize the burden on businesses. That is an important goal and should not be ignored in the implementation phase.

Despite a host of concerns with the CCPA statute generally regarding definitions, scope, and aggressive implementation timelines, the majority of our comments are provided under the specific lens of (1) Government Code § 11349 and (2) the overall high burden placed on dealers by various sections of the regulations.

I. Notice at Collection of Personal Information: § 999.305(a)(3) is burdensome and lacks authority.

Section 999.305(a)(3) states the following:

> *A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. 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 the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.*

Requiring businesses to obtain explicit consent from a consumer to use the consumer's personal information for any purpose other than that disclosed in the notice at collection lacks authority.

Civil Code Section 1798.100(b) provides:

> *...A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.*

As evidenced above, the CCPA statute mandates that businesses must provide *notice* to consumers when they wish to use the consumer's personal information for any purpose other than that disclosed in the notice at collection, but does not provide authority to mandate businesses to obtain *explicit consent* from consumers before using their personal information in this way.

Creating this extra mandate, not authorized by the statute, is overly burdensome on businesses who may decide to institute new business practices or programs. After a business provides consumers with notice about plans to use their information in new and/or different ways, a consumer at that point would have the ability to opt out of that new and/or different use.

II. Notice at Collection of Personal Information: § 999.305(d)(2)(b) is burdensome, unnecessary, unclear, and lacks authority.

Section 999.305(d)(2)(b) states the following:

> *(d) A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer, but before it can sell a consumer's personal information, it shall do either of the following:*
>
> *(1) Contact the consumer directly to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out in accordance with section 999.306; or*
>
> *(2) Contact the source of the personal information to:*
>
> *a. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b); and*
>
> *b. Obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice. Attestations shall be retained by the business for at least two years and made available to the consumer upon request.*

Requiring businesses that do not collect information directly from consumers to obtain signed attestations from the source of the personal information describing how the source gave the notice at collection, and having to retain those attestations for two years, is unnecessary, unclear, and lacks authority.

Dealers receive consumer information from many different types of organizations in their day-to-day business practices: vehicle manufacturers, lead generation providers, marketing firms, and outside vehicle repair specialists, just to name a few. Even within each individual organizations' business practices, how they gather customer data may vary widely. Customer information may be gathered via telephone, webform, text message, in-person interactions, surveys, Internet activity... the list goes on. Having to track exactly what medium an individual customer's information was received in is overly burdensome.

In addition, the language is unclear: does the regulation aim to require organizations to disclose whether they gave the notice verbally, in writing, via text message, or online? Or is this signed attestation supposed to gather different information regarding how the notice was given? There is no authority for this proposed requirement within the CCPA statute.

III. Notice of Right to Opt-Out of Sale of Personal Information: § 999.306(a)(1) is unnecessary, unclear, and lacks authority.

Section 999.306(a)(1) states the following:

> *The purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells (or may in the future sell) their personal information to stop selling their personal information, and to refrain from doing so in the future.*

Expanding the "Purpose and General Principles" of the Notice of Right to Opt-Out from a business that sells personal information to businesses that ***may in the future*** sell personal information is unnecessary, unclear, and lacks authority.

Civil Code Section 1798.120(a) provides:

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

The purpose of the notice of right to opt out of the sale of a consumer's personal information is to provide a concrete consumer protection. Expanding that purpose to cover businesses that do not currently sell consumers' personal information but may in the future change their business practices and start selling (or sharing) that information is unnecessary. Once a business starts selling consumer information, they would fall under this provision at that point, and would be covered. The need for this addition to the law is unclear and unsupported by the statute.

IV. Notice of Right to Opt-Out of Sale of Personal Information: § 999.306(b)(2) lacks authority.

Section 999.306(b)(2) states the following:

> *A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods include, but are not limited to, printing the notice on*

> *paper forms that collect personal information, providing the consumer with a paper version of the notice, and posting signage directing consumers to a website where the notice can be found.*

Directing businesses that substantially interact with consumers offline to also provide notice to the consumer by an offline method lacks authority.

Civil Code Section 1798.130(a)(1) provides:

> *(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:*
>
> > *(1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.*

Because the CCPA statute does not provide for this third offline method, Section 999.306(b)(2) should simply mirror the privacy policy language in Section 999.308(a)(3), which states that:

> *A business that does not operate a website shall make the privacy policy conspicuously available to consumers.*

Dealers are already mandated under a bevy of state and federal laws to provide scores of consumer forms and signs. At the very least, it would be less burdensome to have the ability to direct a consumer's in-person request to a computer terminal at the dealership so the consumer can utilize the interactive webform already mandated by statute.

V. Notice of Right to Opt-Out of Sale of Personal Information: § 999.306(d)(2) lacks authority.

Section 999.306(d)(2) states the following:

> *(d) A business is exempt from providing a notice of right to opt-out if:*
>
> > *(1) It does not, and will not, sell personal information collected during the time period during which the notice of right to opt-out is not posted; and*
> >
> > *(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.*

Unilaterally creating the rule that 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 is not included in the CCPA statute and lacks authority.

VI. Notice of Right to Opt-Out of Sale of Personal Information: § 999.306(d)(2) contains a grammatical error.

Section 999.306(d)(2) states the following:

> *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.*

The sentence highlighted above contains an extra "that", which should be deleted.

VII. Notice of Financial Incentive: § 999.307(b)(5)(a) & (b) are burdensome, unnecessary, and unclear.

Section 999.307(b)(5)(a) & (b) state the following:

> *(b) A business shall include the following in its notice of financial incentive:*
>
> *(1) A succinct summary of the financial incentive or price or service difference offered;*
>
> *(2) A description of the material terms of the financial incentive or price of service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference;*
>
> *(3) How the consumer can opt-in to the financial incentive or price or service difference;*
>
> *(4) Notification of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and*
>
> *(5) An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including:*
>
> *a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and*
>
> *b. A description of the method the business used to calculate the value of the consumer's data.*

Requiring businesses to calculate the value of a consumer's data, tell consumers how they calculated the value of the consumer's data, and provide a good-faith estimate of the value of a consumer's data is burdensome, unnecessary, and unclear.

The proposed requirement regarding calculation of value is vague. Requiring businesses to both provide a good-faith estimate of the value of a consumer's data *and* require businesses to describe the methodology they used to calculate the value of the consumer's data seem to be in conflict. A good-faith estimate connotes a certain level of vagueness, while a calculation connotes a certain level of mathematical certainty. A calculation seems more onerous in nature than a good-faith estimate.

In addition, the methodology by which a business could undertake this calculation is burdensome and unclear. How do you attach a theoretical dollar amount to a potential vehicle sale transaction or a potential vehicle service event due to consumer information that is maintained for marketing purposes? Plus, this calculation could be different for each person: have they bought a car from the dealer before? Did they buy a high-value vehicle? Do they have family members who may also have vehicle-related needs? The list of possibilities here seems endless. We understand the need to put some value quotient on consumer data in accordance with the CCPA statute, but Implementation of the CCPA as a whole is already going to be incredibly burdensome for businesses, and the way this section is drafted adds an unnecessary level of administrative headache on top of existing issues.

VIII. Privacy Policy: § 999.308(b)(8) contains a grammatical error.

Section 999.308(b)(8) states the following:

> *If subject to the requirements set forth section 999.317(g), the information compiled in section 999.317(g)(1) or a link to it.*

We want to point out that the word "in" should be added between "forth" and "section", above.

IX. Methods for Submitting Requests to Know and Requests to Delete: § 999.312(f)(1) & (2) are burdensome, unclear, and lack authority.

Section 999.312(f)(1) & (2) state the following:

> *(f) 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.*

Requiring businesses to (1) treat deficient consumer requests as if they had been submitted correctly or (2) respond to deficient consumer requests and give specific directions on how to remedy deficiencies in the request is burdensome, unclear, and lacks authority.

There are many ways in which a consumer request could be deficient. This could involve lack of identifying information, lack of clarity about what is being requested, and submitting a request in a manner not contemplated by the CCPA statute. Expecting busy business owners and employees to be able to read a consumer's mind and divine what they are asking, when that request is patently unclear, is overly burdensome and constitutes an unfair requirement.

X. Responding to Requests to Know and Requests to Delete: § 999.313(b) is unclear.

Section 999.313(b) states the following:

> *Businesses shall respond to requests to know and requests to delete within 45 days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If necessary, businesses may 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 request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.*

Requiring businesses to respond to requests to know and requests to delete within 45 days, regardless of time required to verify the request, is unclear. What if more information is needed and the consumer does not follow up with that necessary information? Businesses need to be afforded some mechanism here to be able to treat such a request as if it is deficient.

XI. Responding to Requests to Know and Requests to Delete: § 999.313(c)(1) lacks authority.

Section 999.313(c)(1) states the following:

> *For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).*

Requiring businesses to evaluate a denied request for specific pieces of information and instead treat the request as if the consumer is seeking the disclosure of categories of personal information is not provided for by the CCPA statute and lacks authority. Instead, the request should simply be granted or denied.

XII. Responding to Requests to Know and Requests to Delete: § 999.313(d)(1) lacks authority.

Section 999.313(d)(1) states the following:

> *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.*

Requiring businesses to evaluate an unverifiable request as if the consumer is requesting to opt-out of sale is not provided for under the CCPA statute and lacks authority. If a request is unverifiable, the process should stop once the business notifies the consumer that the request was unverifiable.

XIII. Responding to Requests to Know and Requests to Delete: § 999.313(d)(4) is burdensome, unclear, and lacks authority.

Section 999.313(d)(4) states the following:

> *In its response to a consumer's request to delete, the business shall specify the manner in which it has deleted the personal information.*

Requiring a business to specify how it has deleted personal information in response to a consumer's request to delete is burdensome, unclear, and lacks authority.

Civil Code Section 1798.105(c) provides:

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

Notably, the Civil Code section above contained within the Right to Deletion does not mandate businesses to inform consumers of the manner in which they have deleted the consumer's personal information. Additionally, this proposed mandate is unclear, and businesses will have trouble deciphering what the directive actually *is* on a practical level when it comes to disclosing the "manner" of deletion.

Our dealer members would prefer the ability to reply in a generic manner because different systems will handle data deletion requests differently: for example, marketing systems would delete the consumer's data, transactional systems (where the consumer's data is tagged as "transactional" and thus not subject to deletion) would not delete the consumer's data, and in many reporting systems dealers may be de-identifying the stored data and so that data would not be subject to deletion.

It will be burdensome if, for every separate consumer request, dealers will need to have a custom email response after each separate system verifies the consumer and necessary action is taken (or not taken due to an exception). Dealers, especially those with many different rooftops, would appreciate the opportunity to automate responses as much as possible.

In addition, there is no allowance in this section for situations where data cannot be deleted.

XIV. Responding to Requests to Know and Requests to Delete: § 999.313(d)(5) is unnecessary and lacks authority.

Section 999.313(d)(5) states the following:

> *In responding to a request to delete, a business shall disclose that it will maintain a record of the request pursuant to Civil Code section 1798.105(d).*

Requiring a business to disclose that it will maintain a record of a deletion request pursuant to Civil Code Section 1798.105(d) is unnecessary and lacks authority. Although Civil Code Section 1798.105(d) is referenced, this section does not include a mandate to maintain records of requests or disclose to consumers that they maintain records of requests. In addition, it is unclear how these requests are supposed to be maintained, especially if consumer data is deleted and so the request cannot be linked to a consumer record.

XV. Service Providers: § 999.314(c) is unclear.

Section 999.314(c) states the following:

> *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. A service provider may, however, 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 detect data security incidents, or protect against fraudulent or illegal activity.*

Barring a service provider from using personal information received from a consumer's direct interaction with the service provider for the purpose of providing services to another entity is unclear.

I assume that I understand the intent here – do not allow service providers to take data from one source and then use it for an unconnected, separate purpose. However, as written, this section appears to negate the "business purpose" exception under the CCPA. We would recommend clarifying this section to make the intent clearer.

XVI. Requests to Opt-Out: § 999.315(a) & (b) lack authority.

Section 999.315(a) & (b) state the following:

> *(a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, 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. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and 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.*
>
> *(b) A business shall consider the methods by which it interacts with consumers when determining which methods consumers may use to submit requests to opt-out, the manner in which the business sells personal information to third parties, available technology, and ease of use by the average consumer. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.*

Requiring a business to provide two or more designated methods for submitting requests to opt-out lacks authority. Civil Code Section 1798.135 mandates businesses to provide an opt-out link on Internet homepages, but does not provide for additional opt-out methods as described in Section 999.315(b).

XVII. Requests to Opt-Out: § 999.315(c) is burdensome and lacks authority.

Section 999.315(c) states the following:

> *If a business collects personal information from consumers online, the business shall 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 submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.*

Requiring a business that collects personal information from consumers online to treat user-enabled general browser privacy controls as valid requests to opt out submitted pursuant to Civil Code Section 1798.120 is burdensome and lacks authority.

If the regulations are attempting to cover tech companies that regularly track consumers' browsing data, they need to be narrowly tailored as such. As written, this section does not give consumers meaningful choice and covers *all* businesses. This change in the law is not authorized under the CCPA statute.

In addition, this section assumes that all computer systems and tracking mechanisms are compatible, which may not be the case.

XVIII. Requests to Opt Out: § 999.315(f) is burdensome, unnecessary, and lacks authority.

Section 999.315(f) states the following:

> *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.*

Requiring businesses to notify consumers once an opt-out request is communicated to third parties is burdensome, unnecessary, and lacks authority.

The CCPA statute only mandates that businesses need to notify consumers of their right to opt out. The statute does not require businesses to then contact the consumer after the opt-out request has been completed to let them know that fact. If a consumer wishes to opt out of a business' sharing of their personal information, that is a strong indicator they wish to minimize their communications with a business. Additional, unnecessary communications from businesses to consumers in this way is burdensome to businesses and unnecessary for consumers.

XIX. Requests to Opt-In After Opting Out of the Sale of Personal Information: § 999.316(a) lacks authority.

Section 999.316(a) states the following:

> *Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.*

Requiring businesses to implement a two-step opt-in process after a consumer has opted out of the sale of personal information is not mandated by the CCPA statute and lacks authority. This requirement is excessive and will be hard for businesses to manage.

XX. Training; Record-Keeping: § 999.317(b) and (c) are unnecessary and lack authority.

Section 999.317(b) & (c) state the following:

> *(b) A business shall maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.*
>
> *(c) The records may be maintained in a ticket or log format provided that the ticket or log 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.*

Requiring businesses to maintain detailed records of consumer requests made pursuant to the CCPA and how the business responded to those requests for 24 months is unnecessary and lacks authority under the CCPA statute.

XXI. Verification for Non-Accountholders: § 999.325(e)(1) contains two grammatical errors.

Section 999.325(e)(1) states the following:

> *If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if the business maintains the consumer's name and credit card number, the business may require the consumer to provide the credit card's security code and identifying a recent purchase made with the credit card to verify their identity to reasonable degree of certainty.*

In the highlighted sentence above, the word "identifying" should be changed to "identify". In addition, within the highlighted sentence above, the letter "a" should be added between "to" and "reasonable".

XXII. General Requests.

1) Provide guidance on a business' right to cure and how that process will work.
2) Provide model forms and notices businesses can use to help with compliance efforts.
3) Streamline required notices as much as possible so that consumers are not over-informed at every turn and business compliance is made more manageable.
4) Provide more time for businesses to implement these drastic changes to their day-to-day practices.
5) In cost estimates, account for the need for an attorney or compliance officer to decipher the law's requirements and implement them at a business.
6) Consider classifying vehicle geolocation data as sensitive information that should not be disclosed.
7) If consumer information needs to be shared between businesses for reasonable safety and security purposes (such as vehicle history, safety, & performance), this information should not be subject to opt-out requests.

California's new car dealers understand the state's goals to provide consumers with greater control over how their data is used by businesses. However, the CCPA's overall impact on businesses cannot be overstated. There are over 1,300 franchised new car dealers in the state of California alone, and almost every single one of them will be heavily impacted by the new law. Because of this enormous impact, we appreciate the opportunity provided to provide our comments and feedback on the implementing regulations.

We welcome the opportunity to discuss this series of suggestions further. Please don't hesitate to contact me at [redacted] or [redacted]

Sincerely,

Alisa Reinhardt
Director of Regulatory Affairs, California New Car Dealers Association