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

P 202 371 0910

Writer's direct dial: +1 (202) 408-7407

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