

March 8, 2019

**VIA ELECTRONIC MAIL:** [PrivacyRegulations@doj.ca.gov](mailto:PrivacyRegulations@doj.ca.gov)

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

**RE: Implementing Regulations for the California Consumer Privacy Act of 2018**

Dear Mr. Becerra:

The Network Advertising Initiative (“NAI”) is pleased to submit this letter in response to the Department of Justice’s request for comments regarding implementing regulations it may promulgate under the California Consumer Privacy Act of 2018 (“CCPA”).<sup>1</sup>

**Overview of the NAI**

Founded in 2000, the NAI is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing high standards for data collection and use for digital advertising in multiple media, including web, mobile, and TV.

All NAI members are required to adhere to our FIPPs-based, privacy-protective Code of Conduct (the “NAI Code”), which underwent a revision in 2018,<sup>2</sup> and will be updated again in 2020 to keep up with changing business practices and consumer expectations. Member compliance with the NAI Code is backed up by a strong accountability program, which includes a comprehensive annual review by NAI staff of member companies’ business models, policies and practices to ensure their compliance with the NAI Code, even as their individual businesses, and the industry as a whole, evolves.

Several key features of the NAI Code align closely with the underlying goals of the CCPA, such as the NAI Code’s requirement that NAI members provide consumers with an easy-to-use mechanism to opt out of

---

<sup>1</sup> CAL. CIV. CODE §§ 1798.100 *et seq.*

<sup>2</sup> See NETWORK ADVERTISING INITIATIVE, 2018 NAI CODE OF CONDUCT (2018) [hereinafter NAI CODE OF CONDUCT], [http://www.networkadvertising.org/sites/default/files/nai\\_code2018.pdf](http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf).

Interest-Based Advertising (IBA),<sup>3</sup> its requirement that NAI members disclose to consumers the kinds of information they collect for IBA, and how such information is used.<sup>4</sup> The NAI Code's privacy protections also go further than the CCPA in some respects. For example, the NAI Code includes outright prohibitions against the secondary use of information collected for IBA for certain eligibility purposes, such as credit or insurance eligibility, regardless of whether such information is ever sold, and even when a consumer has not opted out.<sup>5</sup>

The NAI also educates and empowers consumers to make meaningful choices about their experience with digital advertising through its easy-to-use, industry-wide opt-out mechanism.<sup>6</sup>

### **Outline of NAI's Comments**

#### **Part I: Definitions**

- A. The CCPA should be amended, or implementing regulations should clarify, that deidentified information is not personal information.
- B. Regulations implementing the CCPA should clarify that the definition of "sale" applies only when the purpose of a transaction is the exchange of personal information for consideration.
- C. Regulations implementing the CCPA should clarify the application of certain exceptions from the definition of "sale."
- D. CCPA implementing regulations should clarify the circumstances under which probabilistic identifiers also constitute unique identifiers.

#### **Part II: Consumer Exercises of CCPA Rights and Business Responses**

- A. In order to maximize consumer privacy, regulations implementing the CCPA should provide flexibility for how businesses may respond to consumer requests regarding information that has been pseudonymized.
- B. CCPA implementing regulations should clarify that consumers may make specific choices with respect to both opting out of sales of personal information and requesting the deletion of personal information.
- C. CCPA implementing regulations should not prevent businesses from relying on strong verification procedures when responding to consumer requests.

#### **Part III: Disclosure obligations**

- A. CCPA implementing regulations should clarify that a business is not required to disclose the specific pieces of information it has collected about a consumer in its online privacy policy.
- B. CCPA implementing regulations should allow businesses reasonable flexibility regarding the placement of the "Do Not Sell My Personal Information" link.

---

<sup>3</sup> See *id.* § II.C.1.a. The NAI Code of Conduct defines Interest-Based Advertising as "the collection of data across web domains owned or operated by different entities for the purpose of delivering advertising based on preferences or interests known or inferred from the data collected." *Id.* § I.F. Capitalized terms used but not defined herein have the meanings assigned to them in § I of the NAI Code of Conduct. See *generally id.* § I.

<sup>4</sup> See *id.* § II.B.

<sup>5</sup> See *id.* § II.D.2.

<sup>6</sup> For more information on how to opt out of Interest-Based Advertising, please visit <http://optout.networkadvertising.org>.

- C. CCPA implementing regulations should clarify the disclosure requirements associated with third-party sales.
- D. CCPA implementing regulations should clarify the application of the 12-month lookback period.

#### **Part IV: Other issues**

- A. CCPA implementing regulations should clarify that businesses may charge a reasonable fee for goods and services as an alternative to ad-supported goods or services.
- B. CCPA implementing regulations should clarify that businesses are not required to extend their data retention policies to respond to consumer requests.

#### **Part I: Definitions**

##### **A. The CCPA should be amended, or implementing regulations should clarify, that deidentified information is not personal information.**

The original bill that made the CCPA a law<sup>7</sup> was subsequently amended<sup>8</sup> to modify, among other things, the CCPA's definition of "personal information" ("PI") by adding the text bolded below.

*"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following **if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household**[.]<sup>9</sup>*

The addition of the bolded text by the amendment clarifies that the scope of PI should not extend beyond information that "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly" a particular consumer or household.

However, as written, the CCPA lacks clarity in a number of ways that threaten the objectives of the legislation. First, while the law clearly intends for deidentified and aggregate consumer information to fall outside the scope of PI, there could be confusion caused by the structure of the definitions of those terms. Implementing regulations can further promote the CCPA's privacy-protective purposes by ensuring that deidentified information and aggregate consumer information are clearly excluded from the definition of PI. Doing so would promote consumer privacy because it gives businesses an incentive to use deidentified and/or aggregate information instead of PI wherever possible, as businesses would not need to comply with the CCPA's onerous requirements when they take the additional steps required to scrub data in such a way to render it deidentified or by aggregating it.

Indeed, for the same reasons, the CCPA missed an opportunity to further enhance consumer privacy by more strongly incentivizing the use of pseudonymous information by businesses. Business should be incentivized to take the extra steps necessary to use pseudonymous information like cookie IDs and mobile ad IDs (instead of, e.g., clear email addresses or phone numbers), and to avoid associating those pseudonymous identifiers with directly identifying information when processing information about

---

<sup>7</sup> A.B. 375, 2017-2018 Leg. Sess., Reg. Sess. (Ca. 2018).

<sup>8</sup> S.B. 1121, 2017-2018 Leg. Sess., Reg. Sess. (Ca. 2018).

<sup>9</sup> See *id.* § 9 (emphasis added).

consumers. This approach is a common practice in digital advertising and should be leveraged by CCPA implementing regulations to provide an extra degree of privacy protection for consumers. The European Union's General Data Protection Regulation ("GDPR") also recognizes the importance of promoting the use of pseudonymous information, as it relaxes some of its more stringent requirements when businesses make the effort to use pseudonymous information.<sup>10</sup>

However, because the CCPA's definition of PI takes more of an "all or nothing" approach by defining a consumer's social security number on par with cookie IDs, businesses are less likely to take additional steps to rely on pseudonymous consumer information and to avoid associating such data with other PI. We recognize that limiting the scope of what constitutes PI under the CCPA by excluding pseudonymous information likely falls outside the scope of this rulemaking process. Therefore, we are proposing a focus for the implementing regulations to promote privacy-enhancing uses of pseudonymous information. For NAI's specific recommendations on how the CCPA's implementing regulations can encourage the use of pseudonymous information in some circumstances, please refer to § II.A *infra*.

Nonetheless, to avoid ambiguity with respect to deidentified and aggregate consumer information, CCPA implementing regulations should clarify that they are outside the scope of PI. The CCPA defines "deidentified" as follows:

*"Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:*

*(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.*

*(2) Has implemented business processes that specifically prohibit reidentification of the information.*

*(3) Has implemented business processes to prevent inadvertent release of deidentified information.*

*(4) Makes no attempt to reidentify the information.<sup>11</sup>*

Note that both the amended definition of PI and the definition of "deidentified" information are directly keyed to the concept of information that identifies, relates to, describes, is capable of being associated with, or that could be linked, directly or indirectly, to a particular consumer. To be included in the definition of PI, at least one of those conditions must be met. But to fall under the definition of "deidentified" information, none of those conditions may be met. It follows that information meeting the definition of "deidentified" should never fall under the definition of PI. Implementing regulations should clarify that fact.

Proposed Regulatory Language:

*For purposes of paragraph (1) of subdivision (o) of Section 1798.140 of the Act, information shall not constitute "personal information" where such information is deidentified or is aggregate consumer information.*

---

<sup>10</sup> See, e.g., Gabe Maldoff, *Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization*, IAPP (Feb. 12, 2016), <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization>.

<sup>11</sup> CAL. CIV. CODE § 1798.140(h).

**B. Regulations implementing the CCPA should clarify that the definition of “sale” applies only when the purpose of a transaction is the exchange of personal information for consideration.**

Today’s digital economy relies on data flows of all kinds. Indeed, the very structure of the Internet requires the transmission and receipt of data about web browsers, devices, and networks that arguably are PI under the CCPA’s broad definition of the term. While these data flows are critical for many functions of the Internet, they are not accurately characterized as sales of data because the purpose of the transactions wherein those data are transmitted is generally not the exchange of information for monetary consideration. Instead, those data flows are merely the means businesses use to enable functions that are recognized business purposes – for example, loading a webpage or serving a digital advertisement.

Like almost all web-based Internet activity, selecting and serving digital advertisements involves the transmission of information like IP address, user agent, and cookie IDs. However, the purpose of digital advertising is the sale of ad space, not information. For example, if a web browser navigates to a cooking blog funded by advertising, the cooking blog may make a request to an ad-tech partner to serve an ad on the blog. The blog’s request for an ad would be transmitted with a pseudonymous cookie ID such as “AHW32” that distinguishes the browser currently visiting the blog from all other web browsers that have visited the blog. Using this information, the ad-tech company might see that the browser is visiting a cooking site and show an ad for a kitchen appliance, or it might look to the cookie ID and information stored on its servers about the web browser’s online activity, to recognize that “*the browser with cookie ID ‘AHW32’ might be interested in golf,*” and fill the ad space on the blog with an ad for a nearby golf course.

The purpose of the transaction taking place in this example, and others like it, is the sale of ad space from a website to an advertiser, which can occur, and usually does, without identifying a specific individual. The information the ad-tech company may process as an intermediary to the transaction for ad space simply allows, for example, the kitchen appliance manufacturer or golf course to select which web browsers to serve its advertising on more effectively by focusing on audiences who are likely to be interested in their products and services. The CCPA’s implementing regulations should recognize these current realities and privacy-protective practices and seek to encourage them.

However, because the CCPA combines an expansive definition of “sale” with an expansive definition of PI, there is a risk that data processing necessary to complete a sale for ad space could be mischaracterized as a sale of PI, even when such processing does not identify a specific individual. To avoid this result, the CCPA’s implementing regulations should recognize that data processing that is merely an incidental part of a transaction undertaken for another business purpose is not itself a sale of PI under the CCPA.

CCPA defines “sale” as follows:

*“Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.<sup>12</sup>*

We believe the legislature intended this definition of sale to broadly cover any transmission of PI by a business to another business or third party, but only when the transmission takes place *for the purpose* of receiving valuable consideration directly in exchange for that information. By adopting a purpose test that clearly ties the valuable consideration to the PI provided, implementing regulations can look through the complicated structure of data flows to capture true sales, while avoiding overbroad application to data transmissions that, while necessary to complete certain transactions, are merely the means used to affect them. Application of a purpose test to interpret when the CCPA’s definition of “sale” applies would be practical and consistent with other state laws where the “sale” or activity of “selling” is a central focus.

Consider the following illustrative example provided by a Wisconsin Supreme Court case involving the question of when a “sale” takes place for purposes of assessing a sales tax.<sup>13</sup> In that case, the Wisconsin Department of Revenue wanted to collect sales tax from the Milwaukee Brewers baseball organization on the value of the paper admission tickets the Brewers gave to baseball game attendees. The Department’s position was that because the paper tickets were included with the price of admission paid by attendees, they were sold by the Brewers to those attendees.

However, the Court held that the physical admissions tickets provided to attendees of baseball games were not “resold” to those attendees as part of the price of admission, and hence the tickets themselves were not subject to sales tax when given to attendees. This holding demonstrates the idea that something may be a means for completing a transaction without it being the reason why the transaction took place. A purpose test would also correctly decide that the consideration ticketholders paid to the Brewers was given for the purpose of gaining admission to watch a ballgame, not to take possession of a paper ticket.

Proposed Regulatory Language:

*For purposes of § 1798.140(t) of the Act, a business will not be deemed to have sold personal information as part of a transaction when the transmission of such personal information is merely the means used to effect a transaction undertaken for a purpose other than the exchange of personal information for consideration, including, but not limited to:*

*1) the transmission of personal information incidental to the delivery, display, measurement, selection, or analysis of an online advertisement.*

**C. Regulations implementing the CCPA should clarify the application of certain exceptions from the definition of “sale.”**

---

<sup>12</sup> CAL. CIV. CODE § 1798.145(t) (emphasis added).

<sup>13</sup> See Wis. Dep’t of Revenue v. Milwaukee Brewers, 331 N.W.2d 571 (Wis. 1983).

The CCPA exempts from its definition of “sale” the processing of PI in several specific contexts, but these exemptions suffer from ambiguities that could lead to confusion and higher compliance costs. Businesses seeking to rely on these exemptions would benefit from additional clarification on their operation and application. Providing such clarification through implementing regulations will allow businesses to rely on clear exceptions they are entitled to under the law, while reducing the risk of erroneous uses of the exceptions.

1. Exceptions for disclosures at a consumer’s direction.

The CCPA’s first exception from the definition of “sale” covers certain cases where a consumer directs a business to disclose PI to a third party:

*For purposes of this title, a business does not sell personal information when:*  
*(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a third party.<sup>14</sup>*

The application of this exception depends on a consumer’s intent to cause a business to disclose PI about them to a third party. It singles out certain consumer actions that a business may not treat as sufficient to infer a consumer’s intent, but it does not provide any further guidance on what consumer actions a business may rely on to infer intent. To provide clarity, implementing regulations should stipulate certain consumer actions that businesses may rely on as a manifestation of intent.

Proposed Regulatory Language:

*A consumer is deemed to have intentionally interacted with a third party for purposes of § 1798.140(t)(2)(A) if the consumer takes an affirmative action, such as a click or tap, indicating their intent to cause an interaction with that third party.*

2. Exceptions for disclosures to service providers for a business purpose.

Another exception from the definition of “sale” covers certain disclosures of PI by a business to a service provider for a business purpose:

*For purposes of this title, a business does not sell personal information when:*  
...  
*(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.*

---

<sup>14</sup> CAL. CIV. CODE § 1798.140(t)(2)(A).

*(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.<sup>15</sup>*

This application of this exception relies on the operation of two defined terms: “business purpose” and “service provider.” CCPA implementing regulations should clarify how the definition of “business purpose” operates in the context of this exception.

The term “business purpose” is defined as follows:

*“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 . . .<sup>16</sup>*

CCPA implementing regulations should clarify that the list of business purposes included in §1798.140(d)(1)-(7) is not exhaustive. This is an important clarification because there are a range of other legitimate purposes, beyond those specifically identified in the CCPA, for which businesses may need to disclose information to service providers who process such information on their behalf, subject to appropriate contractual restrictions. It is also supported by the CCPA’s text, as the definition of “business purpose” also includes the use of PI for “operational purposes” or other “notified purposes” in addition to the purposes listed in §1798.140(d)(1)-(7).

Proposed Regulatory Language:

*The business purposes specified in §§1798.140(d)(1)-(7) are not exhaustive, and personal information disclosed by a business to a service provider for other operational purposes not specified in §§1798.140(d)(1)-(7) are business purposes if they otherwise meet the requirements of §1798.140. A business that discloses personal information to a service provider for purposes it sets forth in its privacy policy required pursuant to § 1798.130 are disclosures made for a “notified purpose” under §1798.140, and such disclosures are made for a business purpose if they otherwise meet the requirements of §1798.140.*

**D. CCPA implementing regulations should clarify the circumstances under which probabilistic identifiers also constitute unique identifiers.**

The CCPA uses the concept of a “unique identifier” or “unique personal identifier” to inform two other key definitions: that of a covered “consumer” and that of covered “PI.” It is defined as follows:

*“Unique identifier” or “Unique personal identifier” means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number,*

---

<sup>15</sup> *Id.* § 1798.140(t)(2)(C).

<sup>16</sup> *Id.* § 1798.140(d).



*unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, “family” means a custodial parent or guardian and any minor children over which the parent or guardian has custody.*<sup>17</sup>

The definition of “unique identifier” in turn relies in part upon the definition of “probabilistic identifier”:

*“Probabilistic identifier” means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.*<sup>18</sup>

The fact that the CCPA’s definition of PI encompasses probabilistic identifiers is conceptually flawed because these so-called identifiers do not in fact relate to any one unique consumer. An inevitable consequence of including them in the definition of PI is that, in some cases, information associated with them will relate to more than one consumer or device that may, or may not, even be part of the same household. One example for how this may work is a method of serving advertisements to devices based on IP address and user agent.<sup>19</sup> This set of information may relate to a specific device being used by one consumer, but not always. In a workplace setting, for example, computers provided by an employer may all be sharing an IP address, be running the same operating system, and have the same web browser enabled by default. In those circumstances, a probabilistic ID based on IP address and user agent may relate to multiple different coworkers who do not share a household. Clearly this kind of information would not be personal to any one of those coworkers. For the same reasons, probabilistic IDs present problems for consumer access requests – because probabilistic IDs are not directly associated with any one identified consumer, it is not practical for businesses to provide a single consumer with access and deletion rights under the CCPA under these circumstances, or to verify any such consumer requests.

In addition, businesses that use probabilistic identifiers do not necessarily assign a specific degree of probability to the proposition that they identify one particular consumer or device. Instead, many businesses simply make practical assumptions about these identifiers, without making, or even being capable of making, an objective assessment of probability. In those circumstances, implementing regulations should clarify that the mere fact that a business treats a probabilistic identifier as being linked to a unique device or set of devices for practical purposes, such as the serving of tailored advertising, is not sufficient on its own to make it “more probable than not” that the probabilistic ID constitutes personal information.

Proposed Regulatory Language:

*A business will not be deemed to have collected, used, disclosed, sold, or otherwise processed a probabilistic identifier as that term is defined by § 1798.140(p) unless the business has actual knowledge that the identifier identifies a consumer or a device to a degree of certainty of more probable than not.*

---

<sup>17</sup> *Id.* § 1798.140(x).

<sup>18</sup> *Id.* § 1798.140(p).

<sup>19</sup> User agent includes the type of operating system being used (e.g., Mac OS or Windows) and the type of web browser being used (e.g., Safari or Chrome).

## **Part II: Consumer Exercises of CCPA Rights and Business Responses**

### **A. In order to maximize consumer privacy, regulations implementing CCPA should provide flexibility for how businesses may respond to consumer requests regarding information that has been pseudonymized.**

As discussed above, the CCPA's definition of PI has a broad scope that extends much more broadly than just traditional personal identifiers like name and social security number. It also extends substantially beyond the traditional scope of data that is "reasonably linked or linkable" to an identified person. The NAI Code takes a similar approach by extending important privacy protections, including notice and choice, for information associated with pseudonymous identifiers such as cookie IDs and mobile ad IDs.<sup>20</sup> A key feature of the NAI Code is the fact that it tailors its privacy protections to the sensitivity of the information at issue. For example, the NAI Code requires NAI members to offer consumers a choice to opt out of IBA using pseudonymous IDs tied only to a browser or device,<sup>21</sup> but in most circumstances they must obtain opt-in consent for the use of personal identifiers like email addresses, names, or phone numbers for advertising purposes.<sup>22</sup> This tailoring of privacy protections to the sensitivity of data enhances consumer privacy and security by providing an incentive for NAI members to maintain and use only pseudonymous identifiers where possible.

Implementing regulations for the CCPA have an opportunity to similarly enhance consumer privacy and security by providing an incentive for businesses to use pseudonymous information wherever possible. They can accomplish this goal by clarifying that businesses are not required to associate traditional personal identifiers with pseudonymous identifiers or information that has undergone pseudonymization to comply with certain CCPA requirements. Doing so would provide companies an important incentive to avoid using more sensitive information about consumers where possible – a result regulations cannot achieve by taking an "all or nothing" approach and treating a consumer's name, email address, social security number, or other personally identifying information on par with an IP address and unique advertising IDs in all cases.

One area where implementing regulations could accomplish this privacy-protective goal consistent with the intent of the legislature and the text of the CCPA is through the existing exception from certain CCPA requirements when compliance with these requirements would require a business to re-identify or re-link certain information:

*This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that **would be considered** personal information.*<sup>23</sup>

---

<sup>20</sup> Under the NAI Code of Conduct, cookie IDs and mobile ad IDs are considered Device-Identifiable Information (DII), which is defined in part as "any data that is linked to a particular browser or device if that data is not used, or intended to be used, to identify a particular individual." See NAI CODE OF CONDUCT, *supra* note 2, at § I.E.

<sup>21</sup> See *id.* § II.C.1.a. (providing an opt-out choice for Personalized Advertising based on information identified only with particular device or browser).

<sup>22</sup> See, e.g., *id.* § II.C.1.c. (requiring Opt-In Consent for the use of PII to be merged with previously collected DII for Personalized Advertising).

<sup>23</sup> CAL. CIV. CODE § 1798.145(i) (emphasis added).

Implementing regulations should clarify that information maintained by a business in a pseudonymous form is not maintained “in a manner that would be considered personal information.” We note that had the legislature intended to create an exemption from connecting non-PI with PI, it could have used language along the following lines: “This title shall not be construed to require a business to reidentify or otherwise link information that is not personal information.” Instead, we believe the intent of the legislature was to prevent businesses from having to re-link or reidentify information maintained pseudonymously, which would ordinarily not be considered personal information, with traditional identifiers that would be.

Proposed Regulatory Language:

*For purposes of subdivision (e) of Section 1798.100, paragraph (2) of subdivision (d) of Section 1798.110, and subdivision (i) of Section 1798.145 of the Act, information maintained by a business that (i) is deidentified; (ii) is aggregate consumer information; or (iii) has undergone pseudonymization, is deemed not to be maintained by the business in a way that would be considered personal information.*

**B. CCPA implementing regulations should clarify that consumers may make specific choices with respect to both opting out of sales of personal information and requesting the deletion of personal information.**

Section 1798.105 of the CCPA gives consumers the right to request that a business delete any PI about the consumer which the business has collected from the consumer, while § 1798.120 gives consumers the right to opt out of a business’s sale of PI about them.

The statutory language creating those rights is broad and clearly establishes the right of consumers to direct a business to delete all the PI it has collected from them and to direct a business not to sell any of the PI a business has about them. However, the CCPA does not explicitly permit a business to offer a consumer the choice to delete or opt out of a sale regarding some, but not all, types of PI. Regulations implementing the CCPA should clarify that businesses are permitted to offer more specific choices, and that consumers are entitled to receive those choices.

For example, the CCPA gives consumers the right to request that businesses disclose to them the business or commercial purposes for collecting or selling PI about them.<sup>24</sup> If a consumer receives this disclosure from a business, it might specify that the business both collects and sells PI from consumers to (1) offer the product or service to consumers without charging a fee; (2) help advertisers who are interested in reaching consumers to better understand consumers’ interests based on their use of the business’s products or services; and (3) for research purposes that may help the business or a third party improve their products or services. In this example, consumers should be able to specifically direct a business not to sell their PI to a third party for research purposes, while continuing to allow a business to engage in sales to advertisers that enable the consumer to use the product or service without paying a fee.

---

<sup>24</sup> *Id.* § 1798.110(a)(3).

In addition, the CCPA gives consumers the right to request that a business disclose to them the categories of PI it has collected from them.<sup>25</sup> If a consumer receives this disclosure from a business, it might specify that the business has collected (1) email address; (2) full name; (3) postal address; and (4) visual information such as a full-face picture. In this example, consumers should be able to specifically direct a business to delete their full-face picture even if it wants the business to retain the other categories of PI to allow the business to continue communicating with the consumer.

Because the CCPA gives consumers the right to know the different kinds of PI a business has collected about them, as well as the purposes for which the business has collected or sold such information, consumers should be empowered by that knowledge to make specific choices about how businesses collect and use PI about them.

The federal Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act provides a strong precedent supporting more flexible choices for consumers. The CAN-SPAM Act, which requires the provision of an opt-out choice with certain email messages, allows the initiator of such messages to offer recipients the opportunity to choose the specific types of messages the recipient wants to receive or not receive, so long as an option to not receive any commercial electronic mail messages from the sender is also made available.<sup>26</sup>

Proposed Regulatory Language:

- a) *Business compliance with a consumer request for deletion: A business may, in response to a verified consumer request to delete personal information pursuant to subdivision (a) of Section 1798.105 of the Act, present the consumer with a reasonable list of the categories of personal information the business has collected about the consumer along with a reasonable method for the consumer to direct the business to either delete or retain each such category of personal information, provided that the list includes an option under which the consumer may direct a business to delete all of the personal information the business maintains about the consumer.*
- b) *Business compliance with a consumer opt-out request: A business may, in response to a verified consumer request to opt out of the sale of personal information pursuant to subdivision (a) of Section 1798.120 of the Act, present the consumer with a reasonable list of the purposes for which it sells personal information and the categories of third parties to which it sells personal information along with a reasonable method for the consumer to opt out of sales of personal information for each such purpose or category of third party, provided that the list includes an option under which the consumer may choose to opt out of all sales of personal information the business maintains about the consumer.*

---

<sup>25</sup> *Id.* § 1798.110(a)(2).

<sup>26</sup> See 15 U.S.C. § 7704(a)(3)(B) (“More detailed options possible. The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.”).

**C. CCPA implementing regulations should not prevent businesses from relying on strong verification procedures when responding to consumer requests.**

The CCPA requires businesses to take certain actions upon receipt of a “verifiable consumer request” in order to respect various consumer rights granted under the CCPA.<sup>27</sup> The emphasis on verifiable requests is appropriate, as it is critically important for businesses to release PI to a consumer only when that consumer’s identity can be confirmed. The CCPA recognizes this in its definition of “verifiable consumer request.”<sup>28</sup> Unfortunately, the CCPA’s requirements pose challenges for businesses, potentially resulting in a requirement to release PI about a consumer without proper verification. Implementing regulations can help avoid this result and the significant security and privacy risks attending it.

Regulations implementing the CCPA should clarify how businesses may verify consumer requests. However, regulations should not prescribe specific authentication methods that are not sensitive to the size or complexity of a business, or to the type of PI involved in the request. Instead, regulations should provide businesses with flexibility in how they verify consumer requests. This will allow businesses to develop methods that are reasonable with respect to their business processes and the kinds of PI they process, and to avoid the likelihood that any prescribed authentication method may at some time become obsolete or irrelevant.

Allowing flexibility with respect to how businesses verify consumer requests is particularly important because the CCPA prohibits businesses from requiring consumers to create an account for verification purposes.<sup>29</sup> As businesses often verify or authenticate consumers during the course of account formation, this prohibition makes verification more difficult. As such, businesses should have discretion to use reasonable verification methods and exercise caution to avoid disclosing PI when a consumer has not been properly verified.

A clear example of when a business should be enabled to impose more stringent verification procedures is with respect to requests made by an authorized agent on behalf of a consumer.<sup>30</sup> Releasing a consumer’s PI to a person or entity misrepresenting themselves as the consumer’s authorized agent would be an unacceptable privacy and security risk, particularly if such a person or entity is purporting to make access requests on behalf of multiple consumers. Businesses must have the flexibility to rigorously authenticate such requests, or to refuse them if they cannot be satisfactorily verified. Another clear example where more stringent verification procedures are called for is when a business receives a request to disclose specific pieces of PI that are relatively sensitive, such as social security number or other government identifier.

---

<sup>27</sup> See CAL. CIV. CODE §§ 1798.100(c)-(d); 1798.105(c); 1798.110(b); 1798.115(b); 1798.130(a)(2)-(4) (detailing actions a business must take in response to a verifiable consumer request).

<sup>28</sup> See *id.* § 1798.140(y) (“A business is not obligated to provide information to the consumer . . . 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.”).

<sup>29</sup> See *id.* § 1798.130(2) (“The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.”).

<sup>30</sup> See *id.* § 1798.185(a)(7) (referring to access requests made by a consumer’s authorized agent).

Further, implementing regulations should clarify that if a business is unable to verify a consumer request using reasonable methods, the business is not required to obtain additional personal information from a consumer in order to verify the request, and is not required to accept any additional personal information offered by a consumer to verify a request. Instead, regulations should clarify that when a business is unable to verify a consumer request, the business is required only to communicate that fact to the consumer making the request, but it is not required to take any further action with respect to that particular unverified request. Requiring businesses to collect and process additional personal information to verify requests is inconsistent with the goals of the CCPA, as well as the longstanding Fair Information Practice Principle (FIPP) of data minimization.

Finally, implementing regulations should clarify how service providers should respond to access requests and how they interact with businesses for which they provide services in connection with such requests.

Proposed Regulatory Language:

- a) *A business shall establish a reasonable and accessible method for verifying that a consumer making a request to exercise rights under the Act is the consumer about whom the business has collected personal information, or is a person authorized by the consumer to act on such consumer's behalf.*
- b) *If a business cannot verify a consumer's identity based on the information initially provided by the consumer for purposes of verification, then the business shall use a reasonable method to send the consumer, or the person authorized by the consumer to act on the consumer's behalf, an explanation that the business could not verify the consumer's identity and therefore cannot take the action requested by the consumer. A business is not required to request or accept additional personal information from a consumer to verify a consumer request.*
- c) *If a service provider receives a request directly from a consumer, the service provider may respond with an explanation that the consumer's identity could not be verified or that the request should be submitted to the business with the direct relationship with the consumer. The service provider shall, taking into account the nature of the processing and the relationship with the business, upon the business's request, assist the business in fulfilling the business's obligation to respond to the consumer's request, insofar as this is reasonably possible.*

**D. CCPA implementing regulations should provide guidance regarding the extent of business responses to verified consumer requests for disclosure of specific pieces of information.**

The CCPA gives consumers the right to request that a business disclose to them both the categories of PI and the specific pieces of PI the business has collected about them.<sup>31</sup> However, if a business is required to provide voluminous operational data in a “data dump” responding to a request for specific pieces of PI, this would only serve to confuse and overwhelm consumers seeking to obtain only information relevant to the services they receive from a business.

---

<sup>31</sup> See *id.* § 1798.100(a).

To avoid this potential for unhelpful “data dumps,” businesses should not be required to disclose specific pieces of PI the business uses only for its internal operational purposes. Providing operational data to a consumer would not provide a benefit to the consumer commensurate with the costs a business would have to incur to disclose the data.

Proposed Regulatory Language:

*A business is not required to provide specific pieces of personal information that it uses only for its own operational purposes in response to a consumer request under paragraph (5) of subdivision (a) of Section 1798.110 of the Act.*

**Part III: Disclosure Obligations**

**A. CCPA implementing regulations should clarify that a business is not required to disclose the specific pieces of information it has collected about a consumer in its online privacy policy.**

The CCPA gives consumers the right to request that a business provide them with the specific pieces of information it has collected about them, and a corresponding obligation on the business to provide such information to a consumer upon receipt of a verified consumer request.<sup>32</sup>

However, there is some confusion about whether the CCPA also imposes an obligation on a business to disclose the specific pieces of information it maintains about a consumer independently of any verified consumer request by posting such information in its online privacy policy. This confusion arises as follows. Under § 1798.110(c)(5) of the CCPA, a business that collects PI about consumers must disclose the specific pieces of PI it has collected about that consumer “pursuant to” § 1798.130(a)(5)(B), which in turn states:

*(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:*

...

*(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:*

...

*(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.<sup>33</sup>*

The interaction of §§ 1798.110(c)(5) and 1798.130(a)(5)(B) referenced above are confusing because the former appears to require the disclosure of specific pieces of PI in a business’s online privacy policy, while the latter refers only to the disclosure of categories of PI to meet the same requirement. We believe the intent of the CCPA here is to require businesses to disclose only categories PI. A

---

<sup>32</sup> See *id.* § 1798.100.

<sup>33</sup> *Id.* § 1798.130(a)(5)(B).

requirement to publicly disclose specific pieces of PI in an online privacy policy would not be practical for businesses because they not only collect different types of PI from different consumers in many circumstances, but also therefore maintain vastly different sets of specific information across consumers. Publicly disclosing PI in an online privacy policy would also create clear privacy and security risks.

Implementing regulations should resolve this confusion by specifying that a business may comply with § 1798.110(c)(5) of the CCPA by disclosing only the required *categories* of personal information in its privacy policy, and not any specific pieces of PI.

Proposed Regulatory Language:

*A business is deemed to comply with paragraph (5) of subdivision (c) of Section 1798.110 of the Act by disclosing the categories of personal information it collects about consumers pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130 of the Act.*

**B. CCPA implementing regulations should allow businesses reasonable flexibility regarding the placement of the “Do Not Sell My Personal Information” link.**

The language in § 1798.135(a) of the CCPA, coupled with the definition of “homepage” in § 1798.140(l), creates substantial ambiguity as to where the required “Do Not Sell My Personal Information” link is required to appear. Specifically, the definition of homepage is “the introductory page of an Internet Web site and any Internet Web page where personal information is collected.”<sup>34</sup> This is broader than, and inconsistent with, any common definition of a website’s homepage, and it could be interpreted to include any web page engaged in digital advertising, depending on the interpretation of various other provisions of the law.

Additionally, businesses that do not maintain what may be traditionally perceived as a “homepage” would benefit from clarification as to where the required link should be placed in order to best reach consumers. For example, a business should be permitted to place the required link alongside or in conjunction with the link to its privacy policy or page, as that is the location consumers generally visit to learn about their choices and manage any offered privacy preferences.

Proposed Regulatory Language:

*A business shall be deemed in compliance with paragraph (1) of subdivision (a) of Section 1798.135 of the Act where the business places the “Do Not Sell My Personal Information” link on the introductory page of an Internet Web site, or alongside the link to its privacy policy page, or in another clear and prominent position on the business’s Internet Web site or mobile application.*

**C. CCPA implementing regulations should clarify the disclosure requirements associated with third-party sales.**

---

<sup>34</sup> See *id.* § 1798.140(l).



Section 1798.115(d) of the CCPA prohibits a third party from re-selling PI 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 their right to opt out of such re-sale pursuant to §1798.120(a). This provision clearly allows third-party sales of PI if consumers receive appropriate notice and choice. However, the statutory language does not specify who is required to provide such notice and choice to the consumer.

Businesses who sell PI to third parties are well positioned to meet this requirement because they can easily disclose the fact that PI they sell to third parties may then be re-sold by those third parties. They are also well suited to provide an opportunity to opt out of such third-party sales in the disclosures they are required to provide to consumers under § 1798.130 of the CCPA. In contrast, consumers are generally not in a position to interact directly with third parties. CCPA implementing regulations should therefore clarify that the obligations specified in § 1798.115(d) fall upon the business, not the third party to whom the business seeks to sell PI.

In addition, because third parties must rely upon businesses to provide the disclosure required by § 1798.115(d), implementing regulations should clarify that third parties are entitled to rely on contractual assurances by a business that the business has provided consumers with the required notice and choice in advance of a sale.

Proposed Regulatory Language:

*The requirement that a consumer receive explicit notice and an opportunity to opt out of third-party re-sales of personal information pursuant to subdivision (d) of section 1798.115 of the Act shall be met by the business that originally collected the personal information from consumers if such business is seeking to sell such personal information to a third-party re-seller. Third-party re-sellers may rely on contractual assurances from businesses from which they obtain personal information that such businesses have met the requirements of subdivision (d) of section 1798.115 of the Act. Third parties do not have an independent obligation to provide consumers with explicit notice and an opportunity to opt out of third-party re-sales of information pursuant to subdivision (d) of section 1798.115 of the Act when they have obtained such contractual assurances.*

**D. CCPA implementing regulations should clarify the application of the 12-month “lookback” period.**

Section 1798.130 of the CCPA requires in several places that a business provide consumers with information regarding the business’s collection, processing, or sale of PI in the 12 months preceding a consumer request for the same. However, the NAI does not believe that the CCPA’s drafters intended to place compliance obligations on businesses with respect to activity that preceded the Act’s effective date.

Therefore, we recommend that implementing regulations clarify that any 12-month lookback periods a business is subject to under the Act will not extend to any time before the Act’s effective date, or the date on which the implementing regulations take effect.

Proposed Regulatory Language:

*Where a business is otherwise required by the Act to take any action in response to a consumer request with respect to information collected, processed, or sold by the business in the 12 months preceding the business's receipt of a consumer request, a business is not required to take such action with respect to information collected, processed, or sold only before the later of the effective date of the Act or the effective date of these regulations.*

**Part IV: Other issues**

**A. CCPA implementing regulations should clarify that businesses may charge a reasonable fee for goods and services as an alternative to ad-supported goods or services.**

Digital advertising allows websites, mobile apps, and other online platforms and services to provide ad-supported content or services to consumers for free or low-cost. To remain economically viable, online publishers and service providers must be able to charge a reasonable fee, or subscription, as an alternative to offering ad-supported content for those consumers who have exercised their right to opt out of popular data-driven advertising practices used to generate significant revenue. The CCPA recognizes this by explicitly not prohibiting a business “from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer’s data.”<sup>35</sup> However, businesses would benefit from clarification that they can rely on an assessment of fair market value for consumer use of the app, site or service, in lieu of consumer data-driven advertising. It would be unreasonable and impractical to expect companies to derive customized pricing on a per-user basis, depending on a calculated or estimated value of each individual consumer’s data.

Proposed Regulatory Language:

*The requirements of section 1798.125 of the Act shall not be construed to prevent a business from charging a reasonable fee for goods or services as an alternative to free or reduced-cost goods or service supported by advertising.*

**B. CCPA implementing regulations should clarify that businesses are not required to extend their data retention policies to respond to consumer requests.**

Data minimization, including limits on retention of PI, is a critical element of the FIPPs and a common privacy protective practice employed by many companies to minimize the risk of unintended harmful uses of personal and sensitive personal information. The CCPA could conflict with this critical practice due to its lack of clarity regarding obligations for companies to reply to consumer requests.

Specifically, many companies are likely to delete consumer information stored after a period of a few months, while the CCPA places requirements on companies to share information with consumers collected for 12 months prior to a consumer request being made. CCPA implementing regulations should clarify that there is no obligation for a business to retain PI solely for the purposes of fulfilling a

---

<sup>35</sup> *Id.* § 1798.125(a)(2).

consumer request under the CCPA. Although §1798.100(e) of the CCPA states that a business is not required to retain certain PI, implementing regulations should clarify its application to cover all the obligations under the CCPA. Any interpretation to the contrary would create additional privacy and security risks to PI by potentially requiring organizations to retain data longer than they otherwise would.

Proposed Regulatory Language:

*Under no circumstances is a business required to retain PI solely for the purpose of fulfilling a consumer request made under the Act.*

**Conclusion:**

The NAI is grateful for the opportunity to comment on the CCPA rulemaking process. In addition to these comments, we are also including reference materials developed by the NAI that can help illustrate how digital advertising works, and how it benefits both businesses and consumers. If we can provide any additional information or otherwise assist your office as it engages in the rulemaking process, please do not hesitate to contact David LeDuc at david@networkadvertising.org.

\*\*\*\*\*

Respectfully Submitted,

**The Network Advertising Initiative**

BY: David LeDuc  
Vice President, Public Policy

Enclosures