December 6, 2019

VIA ELECTRONIC MAIL: PrivacyRegulations@doj.ca.gov

The Honorable Xavier Becerra
Attorney General
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Proposed Regulations for the California Consumer Privacy Act of 2018

Dear Mr. Becerra:

The Network Advertising Initiative ("NAI") is pleased to submit these comments regarding the regulations proposed for adoption\(^1\) under the California Consumer Privacy Act of 2018 (the "CCPA").\(^2\)

The NAI applauds the efforts the Office of the Attorney General has undertaken to interpret and implement the complex requirements of the CCPA while considering detailed comments from dozens of organizations and individuals in the first phase of this rulemaking process.

The NAI’s aim in providing these comments on the proposed regulations (the “Regulations”) is twofold. First, to identify parts of the Regulations that could be amended to further explain or clarify the proposed requirements. Such amendments would benefit consumers and businesses by promoting compliance with the Regulations. Second, to identify provisions in the Regulations that may conflict with the purpose or intent of the CCPA, and suggest amendments that would bring the Regulations into closer alignment with the CCPA and therefore further the CCPA’s purposes.

\(^1\) **CAL. CODE REGS.** tit. 11, §§ 999.300-341 (proposed Oct. 11, 2019).

\(^2\) **CAL. CIV. CODE** §§ 1798.100 *et seq.*
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 strong privacy standards for the collection and use of data for digital advertising in multiple media, including web, mobile, and TV.

All NAI members are required to adhere to the NAI’s FIPPs-based, privacy-protective Code of Conduct (the “NAI Code”), which has undergone a major revision for 2020 to keep pace with changing business practices and consumer expectations of privacy. Member compliance with the NAI Code is promoted by a strong accountability program, which includes a comprehensive annual review by the NAI staff of each member company’s adherence to the NAI Code, and penalties for material violations, including potential referral to the FTC. Annual reviews cover member companies’ business models, privacy policies and practices, and consumer-choice mechanisms.

Several key features of the NAI Code align closely with the underlying goals and principles of the CCPA. For example, the NAI Code requires members to provide consumers with an easy-to-use mechanism to opt out of different kinds of Tailored Advertising, and requires members to disclose to consumers the kinds of information they collect for Tailored Advertising, and how such information is used. 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 Tailored Advertising 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 of Tailored Advertising.

The NAI also educates consumers and empowers them to make meaningful choices about their experience with digital advertising through an easy-to-use, industry-wide opt-out mechanism.

---

5 See, e.g., id. § II.C.1.a. The NAI Code of Conduct defines Tailored Advertising as “the use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device. Tailored Advertising includes Interest-Based Advertising, Cross-App Advertising, Audience-Matched Advertising, Viewed Content Advertising, and Retargeting. Tailored Advertising does not include Ad Delivery and Reporting, including frequency capping or sequencing of advertising creatives.” Id. § I.Q. Capitalized terms used but not defined herein have the meanings assigned to them by the NAI Code of Conduct. See generally id. § I.
6 See id. § II.B.
7 See id. § II.D.2.
8 For more information on how to opt out of Tailored Advertising, please visit http://optout.networkadvertising.org.
Part I: Definitions

A. The Regulations should be amended to add a definition for the term “webform.”

The Regulations use the term “webform” in several places in connection with the submission of consumer requests through a business’s website or mobile application. In common usage, the term “webform” may be used to denote an online mechanism through which a user may submit information like a name, email address, phone number, and/or demographic information over the Internet. However, because the Regulations contemplate consumers making requests to businesses that may involve only personal information that is not associated with a named actual person, such as a cookie ID, mobile advertising ID, or IP address that the consumer does not know or have easy access to, the common usage of the term “webform” is too limited to allow for consumers to make effective requests in connection with those pseudonymous identifiers.

To avoid confusion and ensure that businesses provide consumers with request mechanisms that are appropriate for the kind of personal information involved in a consumer request, the Regulations should be amended to add a definition for “webform” that allows for flexible and sensible implementations by businesses.

Recommended Amendments to Proposed Regulatory Language:

Section 999.304(w):

“Webform” means any reasonable and easily accessible method made available by a business to consumers for the submission of consumer requests through the business’s website, mobile application, or other internet-connected device. This may include, but is not limited to, interactive buttons, links, tick-boxes, fields for entering personal information, or other reasonable methods that a consumer may use to submit a request to a business.

B. The proposed definition of “categories of third parties” should be amended to clarify that the enumerated categories of companies may be third parties under the Regulations in some contexts, but not others.

As noted in the Initial Statement of Reasons (“ISOR”) accompanying the Regulations, the CCPA requires businesses to disclose to consumers the “categories of third parties with whom the

---

9 See CAL. CODE REGS. tit. 11, §§ 999.306(c)(2); 999.312(a); 999.312(c)(2); 999.315(a) (proposed Oct. 11, 2019).


11 See CAL. CODE REGS. tit. 11, § 999.325(e)(2) (proposed Oct. 11, 2019).
business shares personal information,” but does not define the term “categories of third parties.”

The ISOR also highlights the fact that the proposed definition of “categories of third parties” was drawn from a code of conduct for mobile apps developed in 2013 through the National Telecommunications and Information Administration in the U.S. Department of Commerce. For the mobile app context, the enumerated list of categories of third parties in the proposed definition is illustrative of the kinds of companies that may be third parties where the app itself is the first party.

For example, the user of a mobile app might not understand that the mobile operating system running the app may also collect information about how the user interacts with the app. In that context, because the intent of the user may be to interact directly only with the mobile app, and not with the mobile operating system, it is appropriate to classify the mobile app as a first party and the mobile operating system as a third party. However, as soon as that user exits the mobile app and begins to interact directly with the operating system by scrolling or swiping through other apps the user has installed, the mobile operating system is no longer a third party. Instead, the same mobile app the user has just closed could become a third party if the app continues to collect information about the user’s activity on the mobile device after it has been closed, while the operating system is the first party.

The way users interact with the websites, mobile apps, and other internet-connected services and devices generally involves context shifts similar to the kind described above, so the Regulations should further clarify that the kinds of businesses that should be included as a “category of third party” may change depending on the context in which personal information is collected.

**Recommended Amendments to Proposed Regulatory Language:**

**Section 999.301(e):**

“Categories of third parties” means types of entities that do not collect personal information directly from consumers. Depending on the context in which an entity collects personal information, the types of entities that do not collect personal information directly from consumers may include, but is not limited to:

---


13 Id.

14 See CAL. CODE REGS. tit. 11, §§ 999.301(e) (proposed Oct. 11, 2019) (enumerating advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers).
advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.

Part II: Consumer Exercises of CCPA Rights and Business Responses

A. The provisions in the Regulations regarding methods for submitting requests to know should be amended for clarity and to harmonize with the CCPA.

The Regulations, as currently drafted, would require all businesses to provide a toll-free telephone number as one method through which consumers may make a request to know.\(^\text{15}\) However, the CCPA was amended on October 11, 2019 by Assembly Bill No. 1564.\(^\text{16}\) As amended, the CCPA does not require a business to provide a toll-free telephone number to accept certain consumer requests to know if the business: (1) operates exclusively online; and (2) has a direct relationship with a consumer from whom it collects personal information.\(^\text{17}\) Because the Regulations conflict with the CCPA on this point, the Regulations should be amended to harmonize with the CCPA.

**Recommended Amendments to Proposed Regulatory Language:**

*Section 999.312(a):*

> A business shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business operates a website, this shall include, at a minimum, an interactive webform accessible through the business’s website or mobile application. If the business does not operate exclusively online, or does not have a direct relationship with a consumer from whom it collects personal information, this shall include, at a minimum, a toll-free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

B. Certain requirements in the Regulations regarding business responses to consumer requests to know or delete should be amended for clarity and to harmonize with the CCPA.

1. Provisions in the Regulations regarding the timing of a business’s response to a request to know or delete should be amended to harmonize with the CCPA.

---

\(^\text{15}\) Id. § 999.312(a).


\(^\text{17}\) CAL. CIV. CODE § 1798.130(a)(1).
The ISOR asserts that the CCPA contains two conflicting provisions regarding the maximum time allowed for businesses to respond to a consumer request to know or delete because section 1798.130(a)(2) of the CCPA allows for an extension of the initial 45-day response period by an additional 45 days, while section 1798.145(g) allows for an extension of the initial 45-day response period by an additional 90 days.\(^\text{18}\) The ISOR states that by adopting the 45-day standard from section 1798.130(a)(2) of the CCPA exclusively, the Regulations have clarified the application of conflicting requirements in the statute.\(^\text{19}\)

The NAI does not agree with the characterization in the ISOR of the differing 45-day and 90-day extension provisions in the CCPA as “conflicting.” That is because the 45-day extension period from section 1798.130(a)(2) is available to businesses when “reasonably necessary,” while the availability of the 90-day extension provision in section 1798.145(g) is limited to only when “necessary.” This difference makes it clear that the longer 90-day extension is available to businesses only under a stricter standard of necessity – where the longer extension is “necessary” for a business to process the request. This is in contrast to the 45-day extension period, which is available to businesses under the more flexible standard of “reasonably necessary.”

The language in the Regulations elides this distinction because it uses the 45-day extension period from Section 1798.130(a)(2), while using the “necessary” standard for taking that extension from Section 1798.145(g) (“If necessary, businesses may take up to an additional 45 days to respond to the consumer’s request.”).\(^\text{20}\) This approach appears to conflict with the CCPA, which applies two different standards (“reasonably necessary” vs. “necessary”) for two different extension periods (45 days vs. 90 days). The Regulations should be amended to restore the distinction adopted by the legislature.

In addition, the Regulations should be amended to allow for the initial 45-day period to begin running at the time a business verifies a consumer request. Verifying consumer requests may involve communicating with consumers over time, and businesses cannot control how long it may take consumers to provide information necessary to verify a request.

**Recommended Amendments to Proposed Regulatory Language:**

*Section 999.313(b):*

*Businesses shall respond to requests to know and requests to delete within 45 days of verifying those requests. The 45 day period will begin on the day that the business receives verifies the request, regardless of time required to verify the request. If reasonably necessary, businesses may take up to an additional 45 days to respond to the*

---

\(^{18}\)See ISOR, *supra* note 12, at 17.

\(^{19}\)Id.

\(^{20}\)See CAL. CODE REGS. tit. 11, §§ 999.313(b) (proposed Oct. 11, 2019).
consumer’s request, for a maximum total of 90 days from the day the request is received, verified. If strictly necessary, businesses may take up to an additional 90 days to respond to the consumer’s request, for a maximum total of 135 days from the day the request is verified. In either case, provided that the business must provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

2. The Regulations should be amended to remove provisions that would require businesses to respond to consumer requests in a way that differs from what consumers have actually requested.

The Regulations introduce the novel concept that consumer requests to know or delete made to a business that cannot adequately verify those requests should be assigned a different meaning by the business – for example, by requiring a business to re-interpret a consumer request to delete as a request to opt-out.21 This concept is disconnected from the requirements of the CCPA and at odds with the intent of the consumers making those requests.

The CCPA is grounded in the fundamental principles of notice and choice for consumers. It has extensive transparency and disclosure requirements for businesses and provides consumers with an array of rights that they may exercise with businesses, which are informed by business transparency. Indeed, businesses subject to the CCPA must disclose to consumers all of the rights they may exercise – including requests to know,22 requests to delete,23 and requests to opt out of “sales” of personal information.24 With that information, consumers are empowered to decide which rights to exercise – including a decision to exercise all of them, some of them, or none of them. Forcing companies to impute a different intent to consumers is unnecessary and burdensome for companies with no corresponding consumer benefit. That’s because consumers already have the benefit of being informed about and able to exercise any of the rights granted under the CCPA that they wish with businesses subject to the CCPA.

Further, forcing businesses to re-interpret consumer requests when they cannot adequately verify a consumer’s identity creates new risks for consumer harm. For example, suppose that a consumer has read and understood the privacy policy of a retail website, and understands that the retailer may collect and “sell” the consumer’s personal information in order to offer coupons or discounts on certain goods offered on the website. The consumer accepts the benefit of this bargain and decides not to opt out of “sales” of personal information by the retailer. However, that consumer might eventually find that the discounts and offers she is receiving from the retailer (which may be based on personal information previously collected through the website) are no longer relevant or interesting to her, and decides to make a

21 See id. §§ 999.313(c)(1)-(2); 999.313(d)(1).
22 See CAL. CIV. CODE § 1798.110(c).
23 See id. § 1798.105(b).
24 See id. § 1798.120(b).
request to the retailer to delete her personal information to start with a clean slate, and hopefully receive different discounts and offers based on the use and transfer of personal information collected by the retailer after the deletion request. However, if the retailer is unable to verify the consumer’s request to a reasonable degree of certainty based on the limited personal information it has collected, then under the Regulations, it would have to opt the consumer out of “sale” of personal information. This would thwart the consumer’s intent in this case, as she would stop receiving discounts and offers she wanted to receive when the retailer is forced to treat her request for deletion as a request to opt out of sales.25

Amending the Regulations to remove the requirements for businesses to re-interpret consumer requests would help businesses operationalize their processes for honoring consumer requests without resulting in any downside for consumers, who will still be able to make any request they are entitled to under the CCPA.

Recommended Amendments to Proposed Regulatory Language:

Section 999.313(c)(1):

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

Section 999.313(d)(1):

For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy. The business shall also evaluate the consumer’s request as if it is seeking to opt-out of sale.

---

25 See CAL. CODE REGS. tit. 11, § 999.313(d) (proposed Oct. 11, 2019).
3. The Regulations should be amended to remove the requirement that a business provide a consumer with the specific basis for denying a request to delete.

A business that receives a consumer’s request to delete may have various legally valid reasons for denying that request, in whole or in part. Those reasons may include an inability to adequately verify the identity of the consumer making the request,26 or one or more of nine distinct statutory grounds for denying a request to delete, in whole or in part.27 In cases where a business does deny a request to delete, the Regulations as currently drafted would require the business to inform users about “the basis for the denial, including any statutory and regulatory exception therefor.”28

While providing information about the basis for a denial of a request to delete would promote the consumer’s interest in transparency regarding business retention of personal information subject to a request for deletion,29 that interest should be weighed against the potential burden placed on businesses who may be required to provide customized, detailed responses when denying requests for deletion. Clarifying that a business may provide accurate, general information about why the business may have denied a request to delete would strike an appropriate balance between a consumer’s interest in transparency and the operational burdens imposed on businesses.

Recommended Amendments to Proposed Regulatory Language:

Section 999.313(d)(6)(a):

(6) In cases where a business denies a consumer’s request to delete the business shall do all of the following:

a. Inform the consumer that it will not comply with the consumer’s request and describe the general basis for the denial, including any statutory and regulatory exceptions the business may have relied up when denying the request therefore.[.]”

C. Certain requirements in the Regulations regarding requests to opt-out should be amended to harmonize with the statutory language established by the CCPA, to establish greater clarity, and to ensure that consumer choices are honored.

1. The Regulations should be amended to clarify that a business may verify that an individual making a request to opt-out is a “consumer” entitled to make such a request in accordance with the CCPA.

26 See id. § 999.313(d)(1).
27 See CAL. CIV. CODE § 1798.105(d)(1)-(9).
29 See ISOR, supra note 12, at 20.
Although requests to opt out are treated differently from verifiable consumer requests under the CCPA\(^ {30} \) and under the Regulations,\(^ {31} \) businesses should still be permitted to take reasonable steps to ensure that an individual making a request to opt out is a "consumer" under the CCPA entitled to make the request at all (i.e., that the user is a California resident).\(^ {32} \) While some businesses will choose to extend the CCPA’s requirements more broadly and, for instance, comply with an opt out request from a New York resident, businesses are not required to do so under the CCPA. The Regulations should be amended to clarify that fact.

**Recommended Amendments to Proposed Regulatory Language:**

**Section 999.315(h):**

A request to opt-out need not be a verifiable consumer request. However, a business may take reasonable steps to verify that an individual making a request to opt-out is a “consumer” entitled to make that request, as defined by Civil Code section 1798.140(g). In addition, if a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, or not within the scope of the CCPA, the business may deny the request. The business shall inform the requesting party that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or outside the scope of the CCPA.

2. The Regulations should be amended to ensure that user-enabled privacy controls result in businesses honoring consumer choices, not choices made by technology companies seeking to determine the will of consumers.

Under the Regulations, businesses that collect personal information from consumers online would be required to treat “user-enabled privacy controls,” whether in the form of a “browser plugin or privacy setting or other mechanism,” as a valid request to opt out of sales if it communicates or signals the consumer’s choice to opt-out of the sale of their personal information.\(^ {33} \) While the Regulations place appropriate emphasis on the need for controls to be “user enabled,” which is a critical element for signals that purport to express a user’s choice, multiple challenges remain with respect to the effective implementation of user-enabled signals that should be addressed in final regulations.

\(^{30}\) Compare, e.g., Cal. Civ. Code § 1798.100(c) (requiring a business to comply with a consumer request for the categories and specific pieces of information the business has collected about the consumer only upon receipt of a “verifiable consumer request”) with Cal. Civ. Code § 1798.135(a)(4) (requiring a business to honor a consumer’s request to opt out of the sale of personal information without reference to a verifiable consumer request).


\(^{32}\) Cal. Civ. Code § 1798.140(g).

\(^{33}\) Cal. Code Regs. tit. 11, § 999.315(a) (proposed Oct. 11, 2019).
The marketplace for web browsers and extensions currently includes a diverse set of browser-based controls. Some of them are user-enabled, and others operate by default. Most importantly, these various controls seek to accomplish a wide range of objectives, and they do so through different, and evolving, technological approaches. For instance, some consumers install ad-blocking browser extensions because they don’t want to see any ads while browsing the web. Other consumers use browser plug-ins such as Ghostery\textsuperscript{34} to gain greater insights into third-party data gathering. Meanwhile, several browser-makers have embraced technology that automatically, by default, prevents third-party technologies, such as cookies, from operating the way that websites—and users—intend and expect.

Importantly, privacy settings and signaling mechanisms for web browsers and other internet-connected devices (such as mobile devices, connected TVs, and other IoT devices) are diverse and constantly evolving, and help consumers determine how they share personal information used to customize their experiences, deliver specialized content, and deliver tailored advertising. These Regulations are being developed with the benefit of only a snapshot of what technology signals may be developed in coming years. While many are focusing their attention on the world wide web, this is only one medium consumers may use to engage with businesses, share personal data, and exercise their rights under the CCPA.

Given this reality, it is imperative that regulations to implement the CCPA achieve two key objectives: (1) ensure that user-enabled privacy controls represent a clear, informed consumer choice to opt out of “sales” under the CCPA; and (2) remain technology-neutral by prohibiting businesses from using technologies that may inhibit or conflict with signals that express consumer choices to opt out of sales under the CCPA.

First, the final regulations should further clarify that user-enabled privacy controls that businesses are required to treat as valid requests to opt out of sales of personal information must clearly and unambiguously express the meaning of the signals sent by those controls. For example, some consumers choose to install ad-blocking extensions for their web browsers, which may prevent digital ads from loading on web pages that the browser visits. The fact that such a browser extension is installed and activated does not \textit{ipso facto} communicate a consumer’s intent to opt out of sales of personal information, and businesses should not be required to treat them as such. Similarly, a “do not track” signal currently available in some web browsers was never designed for or marketed to users as a tool to for opting out of sales under the CCPA. For that reason, “do not track” signals cannot be expected to communicate to businesses a consumer’s intent to opt out of sales of personal information, and businesses should not be required to treat them as such.

Second, the final regulations should include a provision that prohibits businesses from interfering with or obstructing the function of such user-enabled privacy controls. For example,

\textsuperscript{34} Ghostery, https://www.ghostery.com (last visited Dec. 6, 2019).
existing user-enabled privacy controls for opting out of Interest-Based Advertising in some cases rely on the use of third-party cookies to store user-enabled opt-out choices. Similar mechanisms will be also be available for users to express a choice to opt out of sales under the CCPA. However, certain web browsers such as Safari may automatically delete third-party cookies without differentiating between cookies that store user privacy preferences and those that serve other functions, like analytics or ad customization.35 Web browsers should not be permitted to interfere with a consumer’s CCPA opt-out choices simply because those choices are expressed using third-party cookies.

Recommended Amendments to Proposed Regulatory Language:

Section 999.315(a)

If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that clearly and unambiguously communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer. A business is prohibited from interfering with or stopping the propagation of user-enabled privacy controls that so signal the consumer’s choice to opt-out of the sale of their personal information.

3. The Regulations should be amended to clarify how businesses are required to “act upon” a request to opt out.

As currently drafted, the Regulations would require a business in receipt of a request to opt out to “act upon the request as soon as feasibly possible, but no later than 15 days from the date the business receives the request.”36 The Regulations should be amended to clarify that acknowledging receipt of a request to opt out is sufficient to satisfy the requirement.

Recommended Amendments to Proposed Regulatory Language:

Section 999.315(e):

Upon receiving a request to opt-out, a business shall act upon the request by, at a minimum, acknowledging receipt of the request as soon as feasibly possible, but not later than 15 days from the date the business receives the request.

36 CAL. CODE REGS. tit. 11, § 999.315(e) (proposed Oct. 11, 2019).
4. The Regulations should be amended to remove the requirement for businesses to notify third parties to whom they have sold personal information of a consumer’s opt-out request.

As discussed in other comments above, the core principles of the CCPA are notice and choice. Under the law, consumers are entitled to detailed notice about the ways a business collects and uses personal information, which in turn allows consumers to make informed choices about, e.g., whether to opt out of that business’s sale of personal information, or to request that the business delete the consumer’s personal information. This set of corresponding consumer rights and business obligations is also directional – a consumer has the right to notice and choice from each covered business under the CCPA, and each covered business owes notice and choice to each California consumer. However, the CCPA clearly does not create a general right for consumers to be free from all sales of their personal information from all businesses by default, or obligate businesses to stop selling personal information in the absence of a consumer’s request to opt out.

However, as currently drafted, the Regulations depart from these core CCPA principles when they require each business that receives a request to opt out to notify each third party to whom the business has sold personal information within 90 days of receiving the request to opt out. In turn, each third party that is so notified must opt the consumer out of its sales of personal information, even though the consumer may have never expressed an opt-out choice to those third parties. The ISOR explains that this new requirement in the Regulations is intended in part to address the concern that “consumers may not know the identity of the companies to whom businesses have sold their information in order to make an independent request.” This is a meaningful concern – however, it is mitigated by two important factors that the ISOR does not address.

First, California’s Data Broker Registration bill (AB 1202) became law on October 11, 2019. The express intention of the legislature in drafting this bill included addressing the fact that “consumers are generally not aware that data brokers possess their personal information, how to exercise their right to opt out, and whether they can have their information deleted, as provided by California law,” and that “it is the intent of the Legislature to further Californians’ right to privacy by giving consumers an additional tool to help control the collection and sale of their personal information by requiring data brokers to register annually with the Attorney General and provide information about how consumers may opt out of the sale of their personal information.” The way the bill defines “data broker” covers precisely the kind of

37 Id. § 999.315(f).
38 Id.
39 ISOR, supra note 12, at 25.
41 Id.
scenario the Regulations address in section 999.315(f), i.e., a third party that has obtained personal information from a business, and that may re-sell that information to others. The California legislature was aware of the issue identified in the ISOR, and determined that the appropriate way to promote consumer awareness and exercise of choice was to require “data brokers” to participate in a central registry where consumers may learn about them and subsequently exercise their right to opt out of sales when they decide to do so. Put another way, AB 1202 works in conjunction with the CCPA’s core principles of notice and choice in a way the Regulations do not, because AB 1202 gives consumers a way to know about and opt out of third-party resales of personal information, while the Regulations take that choice out of the hands of consumers, contrary to the spirit of the CCPA. Instead, the Regulations should be amended to require businesses to direct consumers to the new data broker registry (where applicable), which would appropriately address the concerns raised in the ISOR and harmonize with the intent of the legislature without requiring a new set of impractical and extra-legal requirements.

Second, the Regulations would prevent businesses from selling personal information even though a consumer has never expressed a choice to opt out of sales to those businesses. This result is antithetical to the principles of notice and choice. Further, it may upset consumer expectations if it results in an opt out of sales from a business with which the consumer is already familiar and has made an informed choice not to opt out of sales. Directing consumers to the new data broker registry instead will enhance transparency for consumers and provide an effective mechanism for them to learn about third parties and exercise their CCPA rights with those third parties.

In addition, it will be difficult or impossible for businesses to operationalize the requirement to look back 90 days to notify businesses they have sold personal information to and instruct them to stop selling that information.

Finally, the proposed requirement for a business to notify the consumer after notifying third parties to opt that consumer out of sales (although the consumer has made no such request) is burdensome and unnecessary. It does not provide actionable information for consumers and should be removed.

Recommended Amendments to Proposed Regulatory Language:

Section 999.315(f):

A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the consumer’s request

42 “Data broker” means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.” Id.
that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.

If a business knowingly sells a consumer’s personal information to third parties who may further sell such information, the business must provide explicit notice of that fact in its privacy policy and provide a link to the internet web page created by the Attorney General pursuant to Civil Code Section 1798.99.84, and explain that consumers may navigate to that page to learn more about how to exercise their CCPA rights with those third parties.

D. The Regulations should be amended to further clarify how businesses may inform consumers about the method used to comply with requests to delete.

The Regulations, as currently drafted, would require a business to respond to a consumer after honoring their request to delete and “specify the manner in which it has deleted the personal information.” The Regulations should be amended to clarify that businesses should meet this requirement by referring to the deletion methods specified in proposed regulation 999.313(d)(2) (i.e., that the business has either permanently erased, de-identified, or aggregated the personal information), and not by providing consumers with excessive or confusing technical information about, e.g., specific de-identification or aggregation methods the business may have used.

Recommended Amendments to Proposed Regulatory Language:

Section 999.313(d)(5):

In its response to a consumer’s request to delete that the business has verified and completed, the business shall indicate which deletion method it used to delete the personal information pursuant to section 999.313(d)(2). specify the manner in which it has deleted the personal information.

E. The Regulations should be amended to further clarify how the standards for verifying consumer requests apply to businesses that maintain pseudonymous personal information.

The Regulations include detailed provisions pertaining to the verification by a business of consumer requests to know and delete, which have conveyed needed clarity about how businesses may provide (or delete) personal information to consumers who are entitled to it, while maintaining strong security measures and preventing the unauthorized disclosure of personal information.

43 CAL. CODE REGS. tit. 11, § 999.313(d)(5) (proposed Oct. 11, 2019).
However, the Regulations lack sufficient clarity with respect to requirements for businesses to verify requests from consumers in cases where the business maintains only pseudonymous personal information. Therefore, the Regulations should be amended to further clarify how businesses may verify the identity of the consumer making a request, either to a “reasonable degree of certainty” or a “reasonably high degree of certainty,” as applicable. As currently drafted, the Regulations state that a business may match two data points provided by the consumer with data points maintained by a business to achieve a “reasonable degree of certainty,” and three data points to achieve a “reasonably high degree of certainty.” Amendments to the Regulations should clarify that, in both cases, a business is not required to match a minimum number of data points to achieve the requisite degree of certainty, and further that the ability of a business to match such data points does not per se constitute the requisite degree of certainty. Making those amendments will provide businesses with helpful guidelines for reaching the requisite degree of certainty while clarifying that businesses remain responsible for actually achieving those standards, and may not simply rely on a prescriptive number of match points as a proxy for them. This is particularly relevant and important for businesses that do not collect and store multiple pieces of personal information about a consumer, or have a means to correlate previously collected personal information with new personal information supplied in a request. It is also relevant for businesses that only store pseudonymous personal information, and have explicit policies prohibiting the collection and use of personally identifiable information, such as names or email addresses, which may be used to directly identify an individual.

Further, the Regulations should be amended to clarify that the different “certainty” standards apply equally to businesses who maintain pseudonymous personal information about consumers, even though the “matching” process may occur through a fact-based verification procedure instead of matching data points known by the consumer and maintained by the business.

**Recommended Amendments to Proposed Regulatory Language:**

*Section 999.325(b):*

> A business’s compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may, but is not required to include matching at least two data points provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer. Businesses that cannot verify the identity of the consumer making the request to a reasonable degree of certainty after matching two such data points may, but are not required to take further steps to verify the consumer’s

---

44 Id. § 999.325(b).
45 Id. § 999.325(c).
identity, including matching additional data points provided by the consumer, conducting a fact-based verification process, and considering the factors set forth in section 999.323(b)(3).

Section 999.325(c):

A business’s compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may, but is not required to include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Businesses that cannot verify the identity of the consumer making the request to a reasonably high degree of certainty after matching three such data points may, but are not required to take further steps to verify the consumer’s identity, including matching additional data points provided by the consumer, conducting a fact-based verification process, and considering the factors set forth in section 999.323(b)(3). Businesses shall maintain all signed declarations as part of their record-keeping obligations.

Section 999.325(e)(2):

(e) Illustrative scenarios follow:

(2) If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information. This may require the business to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3). When conducting such a fact-based verification procedure, the business still must achieve the degree of certainty required for consumer requests set forth in sections 999.325(b)-(d), as applicable, which may, but is not required to include matching non-name identifying information provided by the consumer with non-name identifying information maintained by the business as set forth in sections 999.325(b)-(d).
Part III: Disclosure Obligations

A. The Regulations should be amended to clarify that businesses required to provide consumers with a “notice at collection” may always provide such notice at or before the time that business collects personal information.

Under the CCPA and the Regulations, a consumer is entitled to receive from a business that collects the consumer’s personal information notice about the categories and purposes of such collection “at or before” the point of collection. This standard allows businesses to provide the required notice either before any collection of personal information, or at the same time that it collects personal information.

However, the Regulations contain one provision that appears to suggest businesses must satisfy this requirement by providing certain notice before the point of collection. This provision disagrees with the standard articulated in the statute and elsewhere in the Regulations. The Regulations should be amended to harmonize all requirements for notice at collection to the “at or before” standard.

Recommended Amendments to Proposed Regulatory Language:

Section 999.305(a)(2)(e):

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

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

B. The requirements in the Regulations for businesses that are not required to provide a “notice at collection” should provide more flexibility to promote compliance.

The regulations proposed to implement section 1978.115(d) of the CCPA would create detailed, prescriptive requirements that dictate how a business that does not collect personal

---

46 See id. §§ 999.301(i), 999.305(a)(1), 999.305(a)(5); Cal. Civ. Code § 100(b).
information directly from consumers must ensure those consumers receive explicit notice and an opportunity to opt out of sales by that business. For example, such a business would be required under the Regulations to contact the source of the personal information to “obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice.”\(^{48}\)

The NAI Code already requires technology companies in its membership that do not interact directly with consumers to take steps to require that the publisher partners they work with, and who do interact directly with consumers, provide notice and choice to those consumers about the collection and use of information about them for Tailored Advertising.\(^ {49}\) In the NAI’s experience, this is often accomplished through contractual agreements. To harmonize with existing and proven industry practices for pass-on notice and choice requirements, the Regulations should clarify that a contractual agreement satisfies the requirement for a “written attestation.”

In addition, there is strong precedent for the use of model notices as a way to promote uniformity and quality of privacy disclosures.\(^ {50}\) This is valuable not only for business efficiency, but also for more consistency for consumers. The Regulations should be amended to clarify that when a business that does not collect information directly from consumers contractually requires the use of model notices, the maintenance of a model notice by that business will satisfy the requirement to keep an example of the notice.

**Recommended Amendments to Proposed Regulatory Language:**

**Section 999.305(d)**

\(d\) A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer, but before it can sell a consumer’s personal information, it shall do either of the following:

(1) Contact the consumer directly to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out in accordance with section 999.306; or

(2) Contact the source of the personal information to:

\(a\).

\(^{48}\) *Id.* § 999.305(d)(2)(b).

\(^{49}\) *See* NAI CODE OF CONDUCT, *supra* note 4, at § II.B.4.

Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b); and

b. Obtain signed attestations from the source, which may include contractual assurances, describing how the source gave the notice at collection and including an example of the notice, which may include model notices when such notices are the method used by the source to provide the required notice at collection. Attestations shall be retained by the business for at least two years and made available to the consumer upon request.

C. The requirement to disclose whether a business sells the personal information of minors under 16 years of age without affirmative authorization should be amended to include a knowledge condition.

The provisions in the Regulations regarding privacy policy disclosures include a requirement that a business disclose whether or not it sells the personal information of minors under 16 years of age without affirmative authorization.51 This provision should be amended to harmonize with the “actual knowledge” condition found in the CCPA’s provisions regarding the sale of the personal information of consumers under 16 years of age.52 Making this change would prevent businesses from being required to make such statements in their privacy policies when they do not have actual knowledge of the statement’s truth or falsity.

Recommended Amendments to Proposed Regulatory Language:

Section 999.305(b)(1)(e)(3):

State whether or not the business sells the personal information of minors consumers the business has actual knowledge are under 16 years of age without affirmative authorization.

D. The Regulations should be amended to remove the new requirement for businesses to post statistics regarding consumer requests.

The Regulations, as currently drafted, create a new requirement not found in the CCPA that would compel certain businesses to provide annual statistics in their privacy policies regarding the number of consumer requests received, complied with, and denied by those businesses.53 Although the ISOR cites potential benefits to the Attorney General, policymakers, academics, and members of the public that could result from this novel requirement,54 those benefits are speculative and in any case disproportionate to the burden that would be placed on businesses

52 See CAL. CIV. CODE § 1798.120(c).
53 See CAL. CODE REGS. tit. 11, § 999.317(g) (proposed Oct. 11, 2019).
54 See ISOR, supra note 12, at 28.
required to compile and provide such statistics. For that reason, the Regulations should be amended to remove this new requirement.

Recommended Amendments to Proposed Regulatory Language:

Section 999.317(g):

(g) A business that alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall:

(1) Compile the following metrics for the previous calendar year: a. The number of requests to know that the business received, complied with in whole or in part, and denied; b. The number of requests to delete that the business received, complied with in whole or in part, and denied; c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and d. The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

(2) Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.

However, if the above disclosure requirements are not removed from the Regulations, the Regulations should still be amended to clarify that a business intending to honor requests to know, delete, or opt-out for individuals other than California “consumers” (e.g., residents of other states) may report statistics based on all requests received by the business, and need not report California “consumer” statistics separately. As a practical matter, many businesses lack the ability to differentiate between California “consumers” and residents of other states, so in many cases businesses will seek to extend the rights granted to “consumers” under the CCPA more broadly to residents of other states. This is a positive outcome for consumers in general. However, given this reality, it is not practical for many businesses to report data for California residents separately.

Recommended Amendments to Proposed Regulatory Language:

Section 999.317(g):

(g) A business that alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall:
(1) Compile the following metrics for the previous calendar year: 
   a. The number of requests to know that the business received, complied with in whole or in part, and denied; 
   b. The number of requests to delete that the business received, complied with in whole or in part, and denied; 
   c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and 
   d. The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

(2) Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.

(3) If a business has received additional requests from individuals other than “consumers” as that term is defined by Civil Code section 1798.140(g), the business is not required to compile or disclose statistics for those requests separately, but may include them in compilations required by subsection (g)(1) and the disclosures required by subsection (g)(2).

Part IV: Other issues

A. The proposed requirement for consumers to provide opt-in consent for a business use of personal information in some circumstances should be removed to harmonize with the CCPA.

The CCPA, as noted elsewhere above, is fundamentally a notice and choice law. The legislature circumscribed the choice that must be provided to consumers to cover the sale by businesses of consumers’ personal information, and set opting out as the standard for the choice required.55 In general, the Regulations are consistent with those principles, but they depart from them significantly with a new opt-in consent requirement that is not based in the statute, and is inconsistent with its general structure.

As currently drafted, the Regulations would require a business to provide notice to consumers and obtain “explicit consent” if the business intends to use the consumers’ personal information for any purpose other than the purposes disclosed in the notice at collection.56 This new requirement conflicts with the general structure of the CCPA in at least two ways. First, while the legislature circumscribed the choice that must be provided to consumers to cover the sale by businesses of consumers’ personal information, the new requirement would create a different consumer choice based on new uses of personal information by a business, even if that new use does not involve any other business or third party, much less a sale. Second, while the legislature set opting out as the default standard for the choice required by

55 Except where the sale involves the personal information of consumers younger the 16 years old. See CAL. CIV. CODE § 1798.120(c).
56 CAL. CODE REGS. tit. 11, § 999.305(a)(3) (proposed Oct. 11, 2019).
the CCPA, the new requirement would set a higher standard of “explicit consent” for certain activities that are not subject to consumer choice at all under the statute.

While the intent of the Regulations to allow consumers to rely on the information provided in the notice at collection\(^{57}\) is a worthy one that the NAI fully supports, the requirements set forth in the Regulations go far afield of the CCPA. The CCPA already allows consumers to rely on the disclosures made by businesses in the notice at collection because, under the statute, a business may not use personal information for new purposes before providing consumer with a new and updated notice at collection.\(^{58}\) In addition, a long-established principle under Section 5 of the FTC Act already prevents businesses from applying changes to their privacy policies retroactively, because doing so would be an unfair act or practice.\(^{59}\) Consumer reliance on previous versions of a notice at collection is already strongly protected.

Further, the likely effect of the proposed “explicit consent” requirement will be to incentivize businesses to massively over-disclose the purposes for which they might at some point use personal information in order to avoid the requirement of obtaining “explicit consent” for any changes, even if they have no current intention of using personal information for those purposes. This would be a net detriment to consumers, who would otherwise have more relevant information about the purposes for which a business currently collects their personal information on which to base a choice about whether to opt out of that business’s sale of personal information.

For these reasons, the Regulations should be amended to remove the requirement for businesses to obtain explicit consent from users before using personal information for new purposes. Even without an “explicit consent” requirement, consumers would still be entitled to notice of any changes, the right to opt out of sales based on any changes, and the ability to rely on business adherence to past notices at collection for previously collected personal information.

**Recommended Amendments to Proposed Regulatory Language:**

**Section 999.305(a)(3):**

_A business shall not use a consumer’s personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer’s_

---

\(^{57}\) See ISOR, _supra_ note 12, at 8-9.

\(^{58}\) “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.” _Cal. Civ. Code_ § 1798.100(b).

\(^{59}\) See, _e.g._, _In re_ Gateway Learning Corp., FTC Docket No. C-4120 at ¶ 14 (F.T.C. 2004) (complaint) (stating that applying material changes to a privacy policy retroactively is an unfair act or practice), https://www.ftc.gov/sites/default/files/documents/cases/2004/12/041228ltr0423047.pdf.
personal information for a purpose that was not previously disclosed to the consumer in
the notice at collection, the business shall directly notify the consumer of this new use
through an updated notice at collection and obtain explicit consent from the consumer
to use it for this new purpose.

B. The Regulations should be amended to harmonize requirements for service providers
with the requirements in the CCPA.

The CCPA permits businesses to share personal information with “service providers”\(^{60}\) in a way
that does not constitute a sale of personal information subject a consumer’s opt-out choice.\(^{61}\)
However, the CCPA restricts the purposes for which a business may share personal information
with service providers to “business purposes.”\(^{62}\)

In order for service providers to carry out contracted-for business purposes, it is necessary in
some circumstances for them to collect and disclose personal information with other entities,
because doing so is integral to the business purpose the service provider was contracted to
carry out for the business. The Regulations recognize this fact when they state that a service
provider may combine personal information received from one or more entities to which it is a
service provider to the extent necessary to detect data security incidents, or protect against
fraudulent or illegal activity,\(^{63}\) which is explicitly recognized as a business purpose under the
statute.\(^{64}\)

However, the Regulations as currently drafted do not allow for the combination of personal
information to perform the other business purposes that service providers are explicitly
permitted to carry out under the statute. Further, the ISOR states without argument that
combining personal information to the extent necessary to detect data security incidents, or
protect against fraudulent or illegal activity is the only activity where the combination of
personal information may be “reasonably necessary and proportionate to achieve the
operational purposes” a service provider has collected personal information to carry out.\(^{65}\) This
broad pronouncement is unjustified, because what data processing activities are “reasonably
necessary and proportionate to achieve an operational purpose” is a fact-specific inquiry that
may vary by business purpose and by the type of business carrying out the activity.

For these reasons, the Regulations should be amended to allow personal information to be
combined for any statutory business purposes, so long as the conditions for remaining a service
provider are otherwise satisfied.

\(^{61}\) Id. § 1798.140(t)(2)(C).
\(^{62}\) See id. § 1798.140(v).
\(^{63}\) Cal. Code Regs. tit. 11, § 999.314(c) (proposed Oct. 11, 2019).
\(^{65}\) ISOR, supra note 12, at 22.
Recommended Amendments to Proposed Regulatory Language:

Section 999.314(c):

A service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity carry out a business purpose as that term is defined by Civil Code section 1798.140(v), pursuant to its service provider contracts.

C. The Regulations should be amended to remove the requirement that a business disclose the value of a consumer’s personal information when a financial incentive is provided.

It is challenging for any business to assign value to a single consumer’s data, and data often gains value when it is aggregated. Consequently, financial incentive programs will more likely be based on a complex calculation of costs to the business and market comparisons. Any number that a business ultimately discloses will not be meaningful to consumers. Further, businesses deploy a wide range of business models that, in many cases, are proprietary. Therefore, requiring a business to disclose its methods and calculations could require disclosure of competitively-sensitive information. The Regulations should therefore be amended to clarify that a business is not required to disclose proprietary or competitively-sensitive information.

Recommended Amendments to Proposed Regulatory Language:

Section 999.307(b)(5):

(b) A business shall include the following in its notice of financial incentive:
(5) An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including:
a. A good-faith estimate of the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference; and
b. A description of the method the business used to calculate the value of the consumer’s data.
(6) Nothing in this section requires a business to include information in its notice of financial incentive that is proprietary or competitively sensitive.
D. The Regulations should be amended to allow information kept for record-keeping purposes to be used for security and anti-fraud purposes.

The Regulations, as currently drafted, prohibit businesses from using information maintained for record-keeping purposes for any other purpose. Limiting the purposes for which a business may use record-keeping information is an important consumer protection. However, the Regulations should clarify that the scope of this requirement is limited to personal information a business maintains for recordkeeping purposes. In addition, personal information businesses obtain for recordkeeping purposes may also be useful for security and anti-fraud purposes. Allowing a security and anti-fraud exception to this requirement could serve a narrow and legitimate business need and pose no discernable risk of consumer harm from secondary uses of the information.

**Recommended Amendments to Proposed Regulatory Language:**

*Personal information maintained by a business for record-keeping purposes pursuant to section 999.317 shall not be used for any other purpose, except for security and anti-fraud purposes.*

**Conclusion:**

The NAI is grateful for the opportunity to comment on the Regulations for the CCPA. 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 Leigh Freund, President & CEO (leigh@networkadvertising.org) or David LeDuc, Vice President, Public Policy (david@networkadvertising.org).

*****

Respectfully Submitted,

The Network Advertising Initiative

BY: Leigh Freund
President & CEO

---