Network Advertising Initiative
409 7th Street NW, Suite 250
Washington, DC 20004

February 25, 2020

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: Modified 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 modifications to the regulations proposed for adoption[1] under the California Consumer Privacy Act of 2018 (the "CCPA").[2]

The NAI appreciates the remarkable effort the Office of the Attorney General ("OAG") has put forth to review thousands of pages of comments submitted by dozens of stakeholders in response to the initial proposed regulations. The modified proposed regulations ("MPRs") clearly represent thoughtful engagement by the OAG with those comments, and they include a number of marked improvements that will promote business compliance with the CCPA.

The NAI has, however, identified certain proposed changes in the MPRs that would benefit from further clarifications and changes, discussed below.

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.

[1] CAL. CODE REGS. tit. 11, §§ 999.300-341 (proposed Feb. 10, 2020).
[2] CAL. CIV. CODE §§ 1798.100 *et seq.*

All NAI members are required to adhere to the NAI's FIPPs-based,[3] 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.[4] Member compliance with the NAI Code is promoted by the NAI's 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 Federal Trade Commission. These 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 and the MPRs. 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,[5] and to disclose to consumers the kinds of information they collect for Tailored Advertising, and how such information is used.[6] The NAI Code's privacy protections also go further than the CCPA and the MPRs 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.[7]

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.[8]

---

[3] *See, e.g.,* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[4] *See* NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020) [hereinafter NAI CODE OF CONDUCT], https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

[5] *See, e.g., id.* § II.C.1.a. The NAI Code 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. *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 MPRs should be amended to clarify when information pertains to a "particular consumer or household."

The MPRs add a new section titled "Guidance Regarding the Interpretation of CCPA Definitions."[9] This section is currently populated only with guidance on the CCPA's definition of "personal information," as follows:[10]

> *Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."*

The NAI welcomes this additional guidance on the definition of "personal information" (and other definitions in the future) and believes businesses will generally benefit from such guidance. Still, this proposed guidance on the definition of "personal information" is generating confusion, because while the CCPA explicitly refers to IP address as a kind of "identifier" and as a "unique personal identifier" that may fall under the definition of "personal information,"[11] the guidance calls the classification of IP address as a form of personal information into question, that is, when it may or may not be considered personal information. Further, because IP address is defined by the CCPA as a type of "unique personal identifier," the guidance also calls into question whether other unique personal identifiers enumerated by the CCPA (such as device identifiers, cookies, beacons, pixel tags, mobile ad identifiers, and even telephone numbers)[12] may also fall outside the definition of personal information in certain circumstances.

The basic source of the confusion generated by the guidance stems from uncertainty around what it means to link an IP address (or another unique personal identifier) to a "particular consumer or household." Intuitively, a business "linking" an IP address to a "particular consumer or household" would involve associating the IP address with other identifiers known by the business to refer to a particular consumer or household. For example, if a business

---

[9] CAL. CODE REGS. tit. 11, § 999.302 (proposed Feb. 10, 2020).
[10] *Id.* § 999.302(a).
[11] *See* CAL. CIV. CODE §§ 1798.140(o)(1)(A) (referring to both "unique personal identifier" and "internet protocol address" as types of personal information); 1798.140(x) (referring to "an Internet Protocol address" as a type of "unique identifier" or "unique personal identifier.").
[12] *Id.* § 1798.140(x).

knows a consumer's full name (referring to a "particular" consumer) and links, or reasonably could link, an IP address with that full name, the IP address would become personal information in the hands of that business. Similarly, a business may know a residential address for a household, and if it links an IP address to the residential address, that would also cause the IP address to be personal information.

The NAI recommends clarifying the guidance on the definition of "personal information" by specifying that information such as an IP address is not personal information unless the business processing such information has linked it, or reasonably could link it, with additional pieces of information known by the business to identify a particular consumer or household, such as name or residential address.

This approach would be largely consistent with the way the NAI Code treats pseudonymous information like an IP address: such information is only considered Personally-Identified Information if it is "linked, or intended to be linked, to an identified individual[.]"[13] This approach places the focus on what a business holding the information does, or actually intends to do with it – not on what may be theoretically possible for any business to do with it. For example, if a news website operator collects IP addresses from website visitors, but does not link IP addresses to any identified individuals (and does not intend to so link them), the IP address is not considered Personally-Identified Information under the NAI Code – even if the same IP address, in the hands of another kind of business like an internet service provider, could be linked to identified individuals.

Recommended Amendments to the MPRs:

Section 999.302(a)

Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any information known by the business to identify a particular consumer or household, such as a full name or residential address, and could not reasonably link the IP address with such information ~~particular consumer or household~~, then the IP address would not be "personal information."

[13] NAI CODE OF CONDUCT, *supra* note 4, at § I.K. Note, however, that IP address is still considered Device-Identified Information and its use is therefore subject to many requirements under the NAI Code, including access to an Opt-Out Mechanism for Tailored Advertising. *See id.* §§ I.E (defining Device-Identified Information); II.C.1.a (requiring an Opt-Out Mechanism for the use of Device-Identified Information for Tailored Advertising).

Part II: Consumer Exercises of CCPA Rights and Business Responses

A. The proposed regulations should not require businesses to disclose precise geolocation information in response to certain consumer requests to know.

The MPRs add a new type of personal information that a business may not disclose in response to a consumer request to know: "unique biometric data generated from measurements or technical analysis of human characteristics."[14] The NAI recognizes that the addition of this type of biometric information by the MPRs was likely in response to the legislature's addition of the same type of biometric information to the list of personal information that, if subject to a data breach, could lead to the exercise of the CCPA's private right of action.[15] This change in the MPRs is consistent with the OAG's reasoning in the Initial Statement of Reasons ("ISORs") as to why certain types of personal information must not be disclosed in response to a request to know (*i.e.*, to "reduce the risk that a business will violate another privacy law, such as Civil Code section 1798.82, in the course of attempting to comply with the CCPA.").[16]

However, the ISORs contain an additional rationale as to why certain types of personal information may not be disclosed pursuant to a request to know, which is balancing "the consumer's right to know with the harm that can result from the inappropriate disclosure of information."[17] Therefore, the MPRs should be further amended under that rationale to include precise geolocation information[18] as a type of personal information businesses may not disclose to consumers who are not accountholders.

The improper disclosure of the precise physical location of a consumer or device over time is potentially very sensitive information. However, the risk of improper disclosure is reduced when a business maintains an account for the consumer making the request because, in that case, the business likely maintains information like an email address and a username/password it may use to securely authenticate a consumer. By contrast, in cases where a business processing precise geolocation information does *not* maintain consumer accounts – *e.g.,* as is the case with a number of NAI members who act as "third party" platforms – the information is

---

[14] CAL. CODE REGS. tit. 11, § 999.313(c)(4) (proposed Feb. 10, 2020).

[15] *See* CAL. CIV. CODE § 1798.81.5(d)(1)(vi) (listing "unique biometric data generated from measurements or technical analysis of human body characteristics" as a form of covered personal information); *id.* § 1798.150(a)(1) (specifying the types of personal information that, if subject to a data breach, support a private right of action).

[16] CAL. DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GEN., INITIAL STATEMENT OF REASONS (ISOR), PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS 18 (2019) [hereinafter ISORs], https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

[17] *Id.*

[18] The NAI Code of Conduct refers to this type of information as "Precise Location Information," defined as "data that describes the precise geographic location of a device derived through any technology that is capable of determining with reasonable specificity the actual physical location of an individual or device, such as GPS-level latitude-longitude coordinates or location-based radio frequency signal triangulation." NAI CODE OF CONDUCT, *supra* note 4, at § I.L.

often held in pseudonymous form only (*e.g.*, associated only with a mobile advertising identifier). This in turn presents unique difficulties for those businesses, because they have no secure way to connect a purely pseudonymous identifier with any particular consumer. There is no way for these third parties to know whether the location information they have pertains to the person who has submitted the request, or whether either the person in possession of a device or the person requesting the information is the actual device owner. These third parties therefore cannot reasonably verify the identity of such users in a manner sufficient to justify providing access to detailed location information – and for reasons of personal privacy and even public safety, the NAI requests that the OAG makes this clear.

This is not merely a hypothetical issue. It is common for a variety of people to have or gain possession of or access to another's mobile device – partners, friends, colleagues or others, whether consensually or not. Any of those persons – whether entrusted by the owner or not – could easily obtain a device ID (from device settings) or take a screenshot of that identifier; if doing so were possible grounds for verifying a request to know, then that person could also obtain the detailed location information of a colleague, spouse, friend or acquaintance. Further, a recent study concluded that approximately one half of mobile phones were not password protected – making the possibility of such "spoofing" a very real concern.[19] Even were a consumer to physically present a mobile device to the business, the business may not be in a position to know if the device is secure (e.g., whether it had a passcode known only by its proper owner/user), or if it has been stolen or otherwise misappropriated.

Moreover, because "third party" platforms (such as NAI members) studiously avoid collecting names, addresses and emails for privacy reasons, they lack those conventional ways to verify the identity of an actual device owner.

Still, consumers in this position would have access to the fact that a business maintains precise geolocation information through the exercise of their right to know the categories of personal information the business maintains,[20] and could still exercise choices with the business about that information (*e.g.*, to opt out of the sale of such information, or to delete it).[21] The exercise of opt out or deletion rights by consumers (with the attending degree of verification required by the MPRs)[22] may adversely affect a business's commercial interests, but unauthorized deletion of precise geolocation information, or opting out of its sale, do not present comparable risks of harm to the consumer as inadvertent disclosure would. Further, the utility of log-level GPS data to consumers is likely minimal (indeed, the NAI is not familiar with any legitimate consumer use cases for such data).

---

[19] *See* Press Release, Kapersky Lab, Kapersky Lab Finds Over Half of Consumers Don't Password-Protect their Mobile Devices (June 28, 2018), https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-finds-over-half-of-consumers-don-t-password-protect-their-mobile-devices.

[20] *See* CAL. CODE REGS. tit. 11, § 999.313(c)(10) (proposed Feb. 10, 2020).

[21] *See id.* §§ 999.315 (pertaining to the right to opt out); 999.313(d) (pertaining to the right to delete).

[22] *See id.* § 999.325.

Due to the considerations discussed above, some businesses processing precise geolocation information only on a pseudonymous basis already believe that they cannot verify the identity of consumers to a reasonably high degree of certainty and would not release precise geolocation information pursuant to a request to know for that reason.[23] But similarly situated businesses remain uncertain of their obligations under the CCPA and the MPRs. To avoid inconsistencies as to how consumer requests to know precise geolocation information are treated, and to protect consumers from the risk of harm from improper disclosure of such information, the MPRs should add precise geolocation information as a type of personal information that businesses may not disclose to non-accountholders in response to requests to know.

Recommended Amendments to the MPRs:

Section 999.313(c)(4):

A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. If a consumer does not have or cannot access a password-protected account with the business, the business shall not disclose in response to a request to know a consumer's precise geolocation information.

B. The proposed regulations should not require businesses to interpret global privacy controls as overriding particular consumer choices.

The MPRs add new provisions that will help businesses understand how they should respond to global privacy controls.[24] In particular, the MPRs make changes ensuring that businesses are only required to treat global privacy controls as valid requests to opt out when those controls clearly communicate that a consumer intends to opt out of sales of personal information (not some other, undefined activity like tracking or advertising), and that global privacy controls represent an affirmative consumer choice, not a default setting.[25] In addition to those helpful clarifications, however, the MPRs also add a new provision requiring businesses to resolve conflicts between local (or site-specific) privacy settings and global privacy settings in favor of the global settings. This new provision does not promote consumer choice and conflicts with longstanding principles regarding how to resolve conflicts between general and specific rules.

Requiring businesses to honor global privacy controls instead of local controls does not promote consumer choice because it does not adequately account for existing preferences

[23] *See id.* §§ 999.325(c), (e)(2).
[24] *See id.* § 999.315.
[25] *Id.* § 999.315(d)(1).

expressed by consumers, and it will create a frustrating, confusing, and repetitive user experience. Consider, for example, the following hypothetical series of events:

1. A consumer visits Website 1, receives a notice of her right to opt out, and she consciously decides not to opt out of sales of personal information by that website in order to support the site.
2. Later, the consumer installs a new browser extension designed to signal a global preference to opt out of sales of personal information. The consumer thinks of this as a default preference, not as one that overrides prior choices.
3. Under the MPRs, a subsequent visit to Website 1 by the consumer would have to be treated by Website 1 as a request to opt the consumer out of sales (because of the presence of a global "do not sell" signal), unless the consumer confirms that she intends **not** to opt out of sales by Website 1.[26]
4. Regardless of how many times the consumer has confirmed her intent **not** to opt out of sales by Website 1, Website 1 would have to surface a confirmation request each time the site encounters that consumer in order to comply with the MPRs as currently drafted. This is because the global setting is always on and will therefore conflict with the existing local preference of the consumer each time the consumer navigates to Website 1 (or any other website where the consumer has expressed a specific preference).

Bombarding consumers with repetitive notices and requests to confirm choices every time they visit known and trusted websites will lead to choice-fatigue and cause consumers to pay less attention to such notices over time. Consumers may instead simply click through without reading or considering privacy notices, a result that does not enhance consumer privacy.

Requiring businesses to override site-specific preferences in favor of global settings could also lead to inconsistent approaches due to continued uncertainty surrounding what global opt-out technologies will become available. This increases the likelihood of non-harmonized and conflicting signals and could create confusion and uncertainty for consumers and business alike. And, although the MPRs require businesses to honor only user-enabled (not default) privacy controls,[27] there are also significant issues around the reliability and authenticity of browser-based signals as well as difficulties clearly communicating which consumers are California residents. Making global settings trump local settings would only exacerbate those problems.

In addition, and irrespective of any notices that may be surfaced to consumers, requiring businesses to honor general settings over particular ones abandons the well-established maxim that if there is a conflict between a general provision and a specific provision, the specific

[26] *See id.* § 999.315(d)(2).
[27] *Id.* § 999.315(d)(1)

provision prevails.[28] This result is counterintuitive and probably does not align with consumer expectations.

Finally, requiring businesses to seek confirmation from consumers of business-specific choices will favor the few large brand advertisers who have direct relationships with consumers and have the ability to ask consumers to override browser or device-setting based opt-out requests. This is dangerous from a competition standpoint, hurting online advertisers' ability to compete as well as potentially reducing revenue for online journalism.

For the reasons discussed above, global privacy settings should govern only where a user has indicated no particular preferences regarding the sales of personal information.

Recommended Amendments to the MPRs:

Section 999.315(d)(2):

If a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the business ~~shall respect the global privacy control but~~ may continue to rely on the existing business-specific privacy setting or the consumer's participation in the financial incentive program ~~notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program~~.

C. The regulations should not require businesses to pass consumer opt-out requests on to any other business for which a consumer has not made an opt-out request.

As the NAI discussed at length in its comments on the initial proposed regulations, the core principles of the CCPA are notice and choice – principles the initial proposed regulations would have departed from had they retained a 90-day lookback for opting out of sales by third parties.[29] Specifically, the initial proposed regulations would have required each business in receipt of a request to opt-out to notify each third party to whom the business had sold personal information within 90 days of receiving the request to opt out, and to require each third party so notified to also opt the consumer out of its sales of personal information for that consumer.[30]

---

[28] *Cf.* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS (1st ed. 2012) (explaining that under the canon *generalia specialibus non derogant*, if there is a conflict between a general provision and a specific provision, the specific provision prevails. While the NAI recognizes that this canon applies literally only to statutory interpretation, it is also useful for inferring intent in other contexts, such as a consumer's intent when their general and specific privacy settings conflict).

[29] *See* Letter from Leigh Freund, President & CEO, Network Advert. Initiative, to Xavier Becerra, Attorney Gen., Cal. Dep't of Justice 13-15 (Dec. 6, 2019), https://www.networkadvertising.org/sites/default/files/final-nai_comment_letter_-_proposed_ccpa_regulations_dec._6_2019.pdf.

[30] *See* CAL. CODE REGS. tit. 11, § 999.315(f) (proposed Oct. 11, 2019).

The MPRs have removed the 90-day lookback found in the initial proposed regulations – a critical adjustment that the NAI strongly supports – but they have replaced it with a different (albeit more limited) lookback period. Specifically, the MPRs would extend the lookback only to the time between the consumer's submission of a request to opt-out and the time a business complies with it.[31]

The more limited scope of the lookback in the MPRs does not, however, resolve other problems with any such lookback. For example, even a more limited lookback still does not take into account the role of the new data broker registry as the primary mechanism through which consumers can exercise their CCPA rights with third parties (such as data brokers) they do not have a direct relationship with. Instead, it would still cause third parties in some circumstances to opt a consumer out of sales of personal information as a matter of law, not pursuant to any actual consumer choice. Instead of forcing third parties to comply with an opt out request a consumer never made, consumers should instead use the data broker registry to identify third parties with whom to exercise their CCPA rights.

In addition, it will be difficult or impossible for businesses to operationalize the requirement to notify businesses they have sold personal information to and instruct them to stop selling that information, even with the more limited lookback to. Consumers are adequately protected by the maximum 15 business day period for complying with valid requests to opt-out.[32]

For those reasons, the MPRs should be amended to remove any lookback requirement for forwarding opt-out requests.

> Recommended Amendments to the MPRs:
>
> *Section 999.315(f):*
>
> *A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.* ~~*If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.*~~

[31] *See* CAL. CODE REGS. tit. 11, § 999.315(f) (proposed Feb. 10, 2020).
[32] *See id.*

Part III: Disclosure Obligations

A. The obligations of businesses that do not collect personal information directly from consumers to provide a notice at collection should be further clarified.

According to the ISORs, the purposes of Section 999.305(d) of the proposed regulations include (1) to clarify that businesses who do not collect personal information directly from consumers (such as data brokers) are not required to provide a notice at collection under certain circumstances; and (2) to provide a way for such businesses to meet their obligations under Civil Code section 1798.115(d).[33]

Reliance by the MPRs on the data broker registry to achieve those purposes represents a more practical approach compared to the one taken by the initial proposed regulations.[34] Relying on the data broker registry is also more closely aligned with the NAI's longstanding approach to consumer transparency and choice around third-party data use, as the NAI operates a central page where consumers can go to learn about Tailored Advertising, and opt out of Tailored Advertising from some or all of NAI's member companies, if they so choose.[35] That said, the language in the MPRs would benefit from further clarification that the provision is intended for businesses that "sell" personal information.

This is an issue because section 999.305(d) of the MPRs as currently drafted removed reference to "sales" by businesses that do not collect information directly from consumers that was present in the initial proposed regulations.[36] However, section 999.305(d) of the MPRs pertains to businesses that are registered as data brokers – who, by definition, sell personal information to third parties.[37] Further, the intent of section 999.305(d) as articulated by the ISORs is to implement Civil Code Section 1798.115(d) – which prohibits a third party from re-selling personal information unless consumers have received explicit notice and an opportunity to opt out.[38] Because the intent of section 999.305(d) still appears to focus on businesses that *sell* personal information, the MPRs should be amended to make it more explicit that section 999.305(d) applies to certain businesses that *sell* personal information; and that it provides a way for those businesses to satisfy their obligations under Civil Code Section 1798.115(d).

---

[33] *See* ISORs, *supra* note 16, at 9-10.

[34] *See* CAL. CODE REGS. tit. 11, § 999.305(d) (proposed Feb. 10, 2020) (relieving businesses of the obligation to provide a notice at collection if they (1) are registered as data brokers and (2) do not collect information directly from consumers).

[35] To opt out of Tailored Advertising or to lean more, visit https://optout.networkadvertising.org.

[36] *Compare* CAL. CODE REGS. tit. 11, § 999.305(d) (proposed Oct. 11, 2019) (referring to steps a business that does not collect information directly from consumers must take "before it can sell a consumer's personal information") *with* CAL. CODE REGS. tit. 11, § 999.305(d) (proposed Feb. 10, 2020) (making no reference to a business's sales of personal information).

[37] *See* CAL. CIV. CODE § 1798.99.80(d).

[38] *See* ISORs, *supra* note 16, at 9-10.

Recommended Amendments to the MPRs:

Section 999.305(d)

If a business that (i) does not collect information directly from consumers and (ii) sells personal information to third parties is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80 et seq., it does not need to provide or take steps to require that the original source of the information provided a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out. A business that satisfies the conditions in this section is deemed to satisfy the requirements of Civil Code section 1798.115(d).

By adopting these recommended amendments, the MPRs will avoid creating a scenario where businesses that don't "sell" personal information are pushed to register as data brokers to meet their obligations under Civil Code Section 1798.115(d).

Part IV: Other issues

A. The proposed regulations should not at this time present a design for an opt-out button.

Under the CCPA, the Attorney General is empowered to establish rules and procedures for the "development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information."[39]

The NAI supports the concept of a uniform logo or button to promote consumer awareness, and has consistently promoted similar industry efforts through the Digital Advertising Alliance's AdChoices Icon, Political Ads Icon, and most recently, the Privacy Rights Icon designed to assist companies with CCPA compliance.[40]

There is, however, a design feature of the button introduced by the MPRs that may cause confusion among consumers and lead to inconsistent adoption among businesses. The proposed design appears to be a toggle – *i.e.*, a privacy control that a user would toggle on or off to either allow or disallow certain activities.[41] However, the MPRs specify that when a user engages the button, it should link out to a webpage or other online location with more information about consumer opt-out rights along with the actual form or method a consumer

[39] CAL. CIV. CODE § 1798.185(a)(4)(C).
[40] *See generally* DIGITAL ADVERTISING ALLIANCE, https://digitaladvertisingalliance.org (last visited Feb. 25, 2020).
[41] *See, e.g.,* The International Association of Privacy Professionals, https://iapp.org (last visited Feb. 25, 2020) (for an example of a true toggle control, navigate to the IAPP website and click the green and white cookie icon on the bottom-left corner of the page).

can use to submit an opt-out request.[42] This creates a conflict between the toggle design of the button and its function as a link to a different location where users can actually exercise control.

This peculiar design feature also points to a potentially broader problem with any future design mandates: because user-interface design is complex, fluid, and often subjective, it is difficult to set useful prescriptive requirements. It would be an undesirable outcome to have a widely-adopted (or even required) standard that is confusing for consumers.

For those reasons, the MPRs should not at this time introduce a design for a "do not sell" button, particularly when industry groups are actively promoting alternative designs that already benefit from marketplace adoption and awareness.[43] Injecting another icon or button option that will likely compete with existing industry icons will likely lead to unnecessary confusion in the marketplace. However, the NAI is supportive of efforts by the OAG to develop a process that would promote the use of a uniform button or logo consistent with Civil Code Section 1798.185(a)(4)(C), without recommending or mandating a specific design.

Recommended Amendments to the MPRs:

Section 999.306(f):

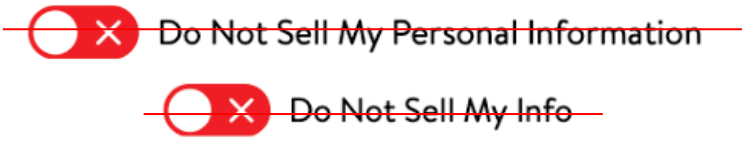
~~*(f) Opt-Out Button*~~

~~*(1) The following opt-out button may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice of right to opt-out.*~~

~~*(2) When the opt-out button is used, it shall appear to the left of the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link as illustrated below, and shall be approximately the same size as other buttons on the business's webpage.*~~

[42] CAL. CODE REGS. tit. 11, § 999.306(f)(3) (proposed Feb. 10, 2020).

[43] *See, e.g.*, *Opt Out Tools,* DIG. ADVERT. ALL., www.privacyrights.info (last visited Feb. 25, 2020) (promoting the CCPA Privacy Rights Icon); IAB PRIVACY, IAB CCPA COMPLIANCE FRAMEWORK FOR PUBLISHERS & TECHNOLOGY COMPANIES VERSION 1.0 8 (2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf (referring to an icon that the IAB may develop for use with its CCPA framework).



~~*(3) This opt-out button shall link to a webpage or online location containing the information specified in section 999.306(c), or to the section of the business's privacy policy that contains the same information.*~~

B. The proposed regulations should further clarify permissible internal uses of personal information obtained in the course of providing services.

Section 999.314(c) of the MPRs helpfully clarifies that a service provider may in some circumstances retain, use and disclose personal information obtained in the course of providing services consistent with its status as a statutory service provider. However, this provision has also generated some confusion as businesses work to understand the scope of permitted activities for service providers.

In particular, businesses are struggling to understand which activities the MPRs intend to cover with the addition of the terms "cleaning" and "augmenting,"[44] as those terms do not have a common meaning in the digital advertising industry and are not defined by the CCPA or the MPRs. Without an established meaning in the industry or clarifying definitions in the MPRs, the introduction of these terms may lead to diverging interpretations and inconsistent application among businesses acting as service providers.

For those reasons, the MPRs should be amended to remove reference to the terms "cleaning" and "augmenting."

Recommended Amendments to the MPRs:

Section 314(c)(3):

A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except . . . [f]or internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles~~, or cleaning or augmenting data acquired from another source~~.

[44] *See* CAL. CODE REGS. tit. 11, § 999.313(c)(3) (proposed Feb. 10, 2020).

Conclusion:

The NAI is grateful for the opportunity to comment on the MPRs. 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