



December 6, 2019

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

Dear Attorney General Becerra,

The protection of the free press is enshrined in the First Amendment to the U.S. Constitution. More than 120 million adults read a daily or Sunday print newspaper. The free press is on the front lines helping the American people hold accountable those who hold positions of power within our democracy and around the world. Digital advertising is a significant source of revenue to media outlets, large and small, and helps keep the press free from government control and affordable. With a well-designed privacy law, the press can continue to do its job as intended in the U.S. Constitution, and consumers can continue to have access to cost-efficient news sources and control of the use and exchange of their personal information.

The News Media Alliance (the “Alliance”) represents over 2,000 media outlets and is composed of nationally recognized organizations, international organizations, and hyperlocal organizations. The Attorney General’s proposed Regulations promulgated pursuant to the California Consumer Privacy Act (“CCPA”), while helpful on a number of levels, impose certain additional burdens on publishers that will render compliance difficult and provide no added benefit to consumers. Indeed, the Regulations may further confuse and convolute consumer control over personal information.

The Alliance believes in giving consumers more transparency and control regarding the use and collection of personal data. In an effort to be more fully compliant with the CCPA and the Regulations and to protect consumer personal information, the Alliance, joined by the California Newspaper Publishers Association, respectfully submits the following comments.

I. The Attorney General Should Clarify the New “Notice at Collection” Requirement.

Section 999.305 imposes new obligations on businesses to make additional disclosures above and beyond the privacy policy when collecting personal information. These new obligations are unclear with respect to what needs to be disclosed, and how, where, and when the notice should be appear.

A. The Attorney General Should Not Require the Posting of a “Notice at Collection” Until January 1, 2021.

The “notice at collection” is a new obligation set forth in the Regulations that is not required by the statute. While the CCPA goes into effect January 1, 2020, the anticipated effective date for the Regulations is sometime before July 1, 2020. The notice at collection obligations were revealed less than three months before the law’s effective date, and they are ambiguous and need clarification.

Because the notice at collection is a new obligation and consumers are likely to see inconsistent implementations that only create confusion, rather than transparency, the Attorney General should clarify that the notice at collection obligation is not effective until January 1, 2021.

B. The Attorney General Should Clarify the Required Placement of the “Notice at Collection.”

The Regulations provide:

The notice [at collection] shall “use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.”¹

Because this is a new obligation and because other requirements such as the “Do Not Sell My Personal Information” button more clearly indicate where and how they should be presented to the consumer, it is difficult for businesses to understand, operationally, how the “notice at collection” should appear and where it should be placed. To remain consistent with existing consumer expectations, the Attorney General should permit businesses to use a link that conspicuously alerts California consumers of the notice on the homepage by being in close proximity to the existing privacy policy link in the website footer or mobile app menu.

C. The Attorney General Should Eliminate Inconsistent Language Regarding the Point in Time When Consumers Must See the “Notice at Collection.”

The Regulations provide:

The notice [at collection] shall...Be visible or accessible where consumers will see it before any personal information is collected.²

This subdivision is inconsistent with the statute³ and even other portions of the Regulations⁴ that permit disclosures regarding privacy practices to happen **at or before** the time of collection.

¹ 11 CCR §999.305(a)(2)(b).

² 11 CCR §999.305(a)(2)(e).

³ CIV. CODE §1798.100(b). “A business that collects a consumer’s personal information shall, *at or before* the point of collection, inform consumers as to the categories of personal

The Attorney General should revise §999.305(a)(2)(e) to be consistent with the CCPA and the other language in the Regulations and provide that the “notice at collection” can be provided **at or before** the time of collection.

II. The Attorney General Should Provide Further Clarification on How to Properly Post the Notice at Collection, Privacy Policy, and “Do Not Sell My Personal Information” Links on Mobile Applications.

The Regulations provide that the notice at collection,⁵ the privacy policy,⁶ and the “Do Not Sell My Personal Information”⁷ links must be conspicuously posted on the mobile application’s download or landing page.

From an operational standpoint, this is problematic because many mobile applications do not have footers, as is the case with actual websites viewed on a device. Often times, the links to the privacy policy and other applicable notices are found in a hamburger menu or gearbox, which consumers have come to associate with being a location for important additional information.

The Alliance requests that the Attorney General clarify that posting the notice at collection, the privacy policy, and the “Do Not Sell My Personal Information” links in the application’s hamburger menu or gearbox will be deemed conspicuous for purposes of by the Regulations.

information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.” (*emphasis added*).

⁴ 11 CCR §999.301(i). “‘Notice at Collection’ means the notice given by a business to a consumer *at or before* the time a business collects personal information from the consumer as required by Civil Code section 1798.100(b) and specified in these regulations.” (*emphasis added*). *See also* 11 CCR §999.305(a)(5) (“If a business does not give the notice at collection to the consumer *at or before* the collection of their personal information, the business shall not collect personal information from the consumer”) (*emphasis added*).

⁵ 11 CCR §999.305(a)(2)(e). “The notice shall...[b]e visible or accessible where consumers will see it before any personal information is collected. For example, when a business collects consumers’ personal information online, it may conspicuously post a link to the notice on the business’s website homepage or the mobile application’s download page, or on all webpages where personal information is collected.”

⁶ 11 CCR §999.308(a)(3). “The privacy policy shall be posted online through a conspicuous link using the word ‘privacy,’ on the business’s website homepage or on the download or landing page of a mobile application.”

⁷ 11 CCR §999.315(a). “A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled ‘Do Not Sell My Personal Information,’ or ‘Do Not Sell My Info,’ on the business’s website or mobile application.”

III. The Attorney General Should Not Require a Notice of Right to Opt-Out of Sale of Personal Information for Businesses Not Currently Selling Personal Information.

The Regulations provide:

The purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells (*or may in the future sell*) their personal information to stop selling their personal information, and to refrain from doing so in the future.⁸

The emphasized portion of this subdivision implies that even businesses that do not currently sell personal information, but may possibly sell personal information in the future, are also required to provide a notice of right to opt-out of sale of personal information. This is inconsistent with the CCPA itself,⁹ which only requires businesses that are currently selling personal information to provide the notice of opt-out of sale of personal information.

The Alliance strongly recommends the Attorney General remove “or may in the future sell” from §999.306(a)(1) of the Regulations in order to avoid consumer confusion. The purpose of the CCPA is to provide transparency with respect to company practices regarding the collection, use, and disclosure of consumer personal information. If any business that does not currently sell personal information but that might theoretically sell personal information in the future is required to provide an opt-out notice, a consumer will never be sure, from the moment that consumer visits a website or sees the notice in a store, whether or not a site is selling personal information.

IV. The Regulations Should Not Require Businesses to Treat Unverified Requests to Delete as Requests to Opt-Out of Sale of Personal Information.

The Regulations provide:

For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.¹⁰

⁸ 11 CCR §999.306(a)(1) (*emphasis added*).

⁹ CIV. CODE §1798.120(b). “A business that sells consumers’ personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the ‘right to opt-out’ of the sale of their personal information.”

¹⁰ 11 CCR §999.313(d)(1)

This new requirement (not found in the statute) to treat an unverified request to delete as a request to opt-out of sale is problematic on multiple levels, most obviously in situations where a business is not selling personal information in the first place, and in situations where the business does not have sufficient information to identify the consumer. There is also a major concern that businesses will be flooded with unverified deletion requests by simply taking names from a telephone book and inputting them into the request for deletion form, or by using an automated bot. The Attorney General should eliminate this requirement.

V. The Attorney General Should Support the Development of Industry Frameworks for a Consistent Opt-Out Approach Under the CCPA And Provide Time for Organizations to Implement Those Frameworks.

Many members of the Alliance are hyperlocal news organizations that cannot afford to build their own opt-out solutions for the CCPA. These businesses welcome the efforts of self-regulatory groups that have been working, across the advertising ecosystem, to develop proposed frameworks to support and facilitate consumer opt-out rights.¹¹ The Attorney General should support these industry efforts and provide additional time for organizations that choose to participate therein to implement those technical specifications.

The BEAR Study included in the Attorney General’s Initial Statement of Reasons points out that the costs associated with developing technological systems to meet the compliance standards of the CCPA are likely to be significant. Even the largest data owners in the world are struggling to figure out how to make the “Do Not Sell My Personal Information” button operational on their platforms, with no long-term viable solution in sight.

Members of the Alliance and others in the advertising ecosystem are engaged in a significant good-faith effort to comply with the CCPA. Given this new legal regime, and the challenges of implementing the opt-out requirements in the ad tech space, the Alliance asks the Attorney General to set forth a compliance grace period for such implementation, up to and including January 1, 2021.

VI. The Attorney General Should Not Restrict a Service Provider’s Ability to Use Information Collected from One Business to Benefit Another Business.

The Regulations provide:

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 service to another person or entity.¹²

¹¹ See, e.g., *IAB CCPA Compliance Framework for Publishers and Technology Companies* (available at <https://www.iab.com/guidelines/ccpa-framework/>).

¹² 11 CCR §999.314(c).

This provision would have severe negative implications for publishers' ability to use any service provider that provides analytic services. Many technology service providers use a single piece of information such as an IP address, received from multiple businesses, to provide services to many different businesses. For example, frequency capping or sequencing functions are extremely helpful to consumers because they limit the number of times consumers see the same ad. Service providers are only able to bring this benefit to consumers if they are able to take information they receive from several businesses and use that information collectively. Another example is Google Analytics. Google Analytics provides a service that allows businesses to track consumer traffic on their websites and mobile applications. It provides insight as to how consumers landed on their website, what consumers did once they were on the website, and how long they stayed on the website. Google Analytics uses all this information from various businesses to provide businesses with online marketing plans that allow them to track and gauge their return on investment in a meaningful way when the Advertising Feature is turned on.

The Alliance recommends the following revised provision:

A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity, **unless the service provider is using the information solely for business purposes and provided those business purposes are disclosed to consumers when responding to requests to know.**

VII. Businesses that Honor Opt-Out Requests Through a “Do Not Sell My Personal Information” Link Should Not Also be Required to Treat the Ad Hoc Use of User-Enabled Privacy Controls as “Do Not Sell” Requests.

The Regulations provide:

If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.¹³

Given the existing requirement that businesses selling personal information include a “Do Not Sell My Personal Information” button on the homepage with direct access to methods to opt-out of the sale of personal information, adding user-enabled privacy controls as another method only exacerbates the complexity facing consumers as they seek to opt-out of sale of personal information. Without a clear delineation between an opt-out of sale and existing user-enabled privacy controls, a consumer may feel he or she must enable and disable privacy-setting controls prior to and after each visit to any number of websites through which he or she does want to

¹³ 11 CCR §999.315(c).

allow the businesses to sell their personal information. This is not the experience consumers want and it does not provide further transparency or control.

Further, under the Regulations as drafted, a business will not know how to reconcile a consumer's use of user-enabled privacy controls with a consumer's action or inaction vis-a-vis a "Do Not Sell" button. In addition, in this scenario, a business has no way to contact a consumer to confirm that it contacted all third parties to which it sold data in the previous 90 days.¹⁴ And if a consumer uses specific user-enabled controls, rather than a global opt-out, a business has no mechanism for contacting the consumer to provide the option to globally opt-out.¹⁵

Additionally, there are currently no standards for "Do Not Track" or other possible browser plug-ins. Requiring publishers to follow various standards created every day is an impossible burden with which small and large publishers will not be able to comply, but which unfairly enhances the power of browser manufacturers.

The Alliance recommends that the Attorney General remove the references to user-enabled privacy controls from the Regulations as they are unnecessary, provide no additional transparency for consumers, and impose undue burdens on businesses.

VIII. The 90-Day Lookback Requirement Exceeds the Scope of the Attorney General's Rulemaking Authority and Should be Eliminated.

The Regulations provide:

A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.

This proposed regulation is problematic for two reasons. First, it would require retroactive application to information collected up to 90 days before the effective date of the CCPA. Second, it would also require retroactive application generally of the do not sell obligation and thereby exceed the scope of the Attorney General's power to regulate. "New statutes are presumed to operate only prospectively absent some clear indication that the Legislature intended otherwise." *Elsner v. Uveges*, 34 Cal. 4th 915, 936 (2004). Here, there is no clear indication that the Legislature intended the do not sell obligation to apply retroactively. Moreover, the statute only requires a prospective obligation on businesses that honor do not sell requests.¹⁶

¹⁴ 11 CCR §999.315(f).

¹⁵ 11 CCR §999.315(d).

¹⁶ CIV. CODE 1798.135(a)(4) and (5). "For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer...[and] respect the consumer's decision to opt-out for at least 12

In order to avoid any retroactive application of the CCPA, the 90-day lookback should be eliminated.

IX. Businesses Should Have 45 Days from the Date a Request to Know or a Request to Delete is Verified to Fulfill or Deny that Request.

The Regulations provide:

Businesses shall respond to requests to know and requests to delete within 45 days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request.¹⁷

There are a number of verification requirements that must be followed for both requests to know and requests to delete. Because of the extensive nature of these requirements, it is clear that each request will need to be verified on a case-by-case basis.¹⁸

The Alliance recommends that the Regulations be revised such that the 45-day window to substantively respond to requests to delete and requests to know begins to run on the day the request is verified.

X. The Attorney General Should Not Require Publication of Metrics in the Privacy Policy for Businesses That Are Required to Maintain Consumer Request Metrics.

The Attorney General has proposed explicit metrics reporting requirements for businesses “that alone or in combination, annually buy[], receive[] for the business’s commercial purposes, sell[], or share[] for commercial purposes, the personal information of 4,000,000 or more consumers.”¹⁹

While the record-keeping requirements are sensible, publication of such metrics is more likely to confuse consumers, particularly if businesses are denying large volumes of frivolous or even fraudulent requests. The numbers themselves will not elucidate for consumers the underlying reasons for the denial, and will only further extend the length of already lengthy privacy policies.

The Alliance would strongly recommend that the Attorney General strike Section 999.317(g)(2) from the Regulations to remove the obligation to post the metrics publicly, and instead require that businesses in this category maintain such records internally and make them available to the Attorney General upon request.

months before requesting that the consumer authorize the sale of the consumer’s personal information.”

¹⁷ 11 CCR §999.313(b).

¹⁸ *See generally* 11 CCR §§ 999.323-999.326.

¹⁹ 11 CCR §999.317(g).

XI. The Attorney General Should Provide Clarity on How Businesses Should Operationalize the Obligation to Provide Aggregated Household Data in Response to Household Requests for Personal Information.

The Regulations provide:

Where a consumer does not have a password-protected account with a business, a business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.²⁰

The average household size is 2.6 people.²¹ It is unclear how any business could provide household information on an aggregated basis for 2.6 people. It is fundamentally inconsistent with the language and the spirit of the CCPA.

In addition, it is unclear whether “household” means any household in the United States or if it is restricted to requests that come from households located in California.

As numerous businesses have pointed out to the legislature and to the Attorney General, allowing one member of a household to obtain information about other individuals in the household – even in “aggregated” form – actually puts the privacy and safety of those household members at risk. The Attorney General should remove subsection (a) and instead require that all consumers of a household jointly request information (as provided in subsection (b)). In the alternative, if the Attorney General is not inclined to remove subsection (a), the Alliance strongly encourages the Attorney General to provide businesses who comply with subsection (a) a safe harbor in the event of a data breach regarding such household information.

The Attorney General should also make clear that this provision of the Regulations is intended to include only those requests received from households located in California.

XII. The Attorney General Should Provide Additional Guidance on the Two Steps Required for Opt-In for Minors, Opting-In After Opting-Out, and Requests to Delete.

The Regulations provide:

For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.²²

²⁰ 11 CCR §999.318(a).

²¹ Pew Research on the Increase in Household Size available at <https://www.pewresearch.org/fact-tank/2019/10/01/the-number-of-people-in-the-average-u-s-household-is-going-up-for-the-first-time-in-over-160-years/>

²² 11 CCR §999.301(a).

A business shall use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.²³

Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.²⁴

This is a new obligation that does not appear in the statute and it lacks substantial compliance guidance. The Attorney General should use this opportunity to provide, at a minimum, examples of sufficient two-step opt-ins. The Alliance provides the following examples of what might be sufficient for purposes of two-step verification:

Example 1: If a business is responding to a verified request to delete via the toll-free number method, the business may ask the consumer to provide an email address. The business will then send a confirmation email to that account for the consumer to confirm they would like their personal information deleted.

Example 2: If a business receives an opt-in request from a minor between 13 and 16 years old via a webform, the business may give the minor an email with a deep link to click onto verify that they would like to opt-in to the sale of personal information.

Example 3: If a business receives a request to opt-in after opting-out via a webform, the business may give the consumer two separate screens – first filling out a request on a webform, and second clicking on a button on a confirmation page that states “confirm my request.”

XIII. The Attorney General Should Provide Guidance on How a Business Can Conclude that Any Given Visitor is a California Resident.

The CCPA and Regulations are both silent regarding how a business determines whether a visitor to a website is a California resident and therefore has certain rights under the CCPA.

The Alliance requests that the Attorney General provide businesses with the ability to use a website visitor’s IP address to determine if such visitor is a California consumer.

²³ 11 CCR §999.312(d).

²⁴ 11 CCR §999.316(a).

XIV. The Attorney General Should Provide Insight into What Constitutes “Reasonable Security” Measures.

The CCPA and the Regulations set forth obligations on businesses, and consequences associated with failing, to provide either “reasonable security procedures and practices” or “reasonable security measures” regarding the transmission,²⁵ verification,²⁶ and protection of personal information.²⁷ However, the Regulations offer no guidance regarding the appropriate standard for reasonable security measures and/or procedures and practices.

The Alliance strongly recommends the Attorney General explicitly set forth in the Regulations that the Center for Internet Security Controls, set forth in the California Attorney General’s 2016 Data Breach Report,²⁸ constitute the applicable baseline standard for reasonable security under the CCPA and the Regulations.

²⁵ 11 CCR §999.313(c)(6). “A business shall use reasonable security measures when transmitting personal information to the consumer.”

²⁶ 11 CCR §999.323(d). “A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer’s personal information.”

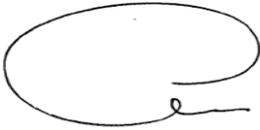
²⁷ CIV. CODE §1798.150(a)(1). “Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following...”

²⁸ *California Data Breach Report*, February 2016, available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>.

XV. The Attorney General Should Offer Regulations on the CCPA Amendments.

Governor Newsom signed additional amendments to the CCPA on October 11, 2019. These included, among other things, a business to business exemption and an employee exemption. Because the amendments were signed after the publication of the Regulations, the Attorney General should promulgate regulations on how to operationalize the above-mentioned exemptions, both of which are scheduled to sunset on January 1, 2021, only six months after the Attorney General begins enforcement of the law.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Chavern', with a large loop at the end.

David Chavern
President & CEO
News Media Alliance