November 8, 2021

regulations@cppa.ca.gov
California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

Re: Comments of the News Media Alliance and California Newspaper Publishers Association in Response to the California Privacy Protection Agency's Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020, PRO 01-21

The protection of the free press is enshrined in the First Amendment to the U.S. Constitution. 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. A vibrant and financially stable independent press is therefore essential to a healthy democracy. The News Media Alliance (the "Alliance") represents over 2,000 media outlets and is composed of nationally recognized media organizations of all sizes ranging from international to hyperlocal.

Digital advertising is a significant source of revenue to media outlets, large and small, and sustains independent journalism by helping to keep the press affordable and free from government control. In the two-and-a-half years since the Alliance submitted comments to then Attorney General Xavier Becerra in connection with the rulemaking under the California Consumer Privacy Act ("CCPA"), journalism has become even more financially vulnerable and more reliant on digital ad revenue for its very existence. When Governor Brown signed the CCPA into law in 2018, digital advertising constituted 49% of journalistic media revenue. In 2020, that share rose to 63%.[1] And while digital revenue is making up a greater portion of total advertising revenue and total revenue, total estimated advertising revenue is actually down, by as much as 29% from 2019 to 2020 by some accounts.[2]

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, as well as control of the use and exchange of their personal information. The regulations ("Regulations") to be promulgated by the newly constituted California Privacy Protection Agency ("CPPA") under the California Privacy Rights Act ("CPRA") will play a significant role in the governance of privacy practices in the digital advertising ecosystem, and provide guidance to other states as

[1] Pew Research Center on Journalism and Media available at https://www.pewresearch.org/journalism/chart/sotnm-digital-and-non-digital-advertising-revenue/

[2] Pew Research Center on Journalism and Media available at https://www.pewresearch.org/journalism/fact-sheet/newspapers/.

they consider their own legal framework.

The Alliance believes in giving consumers more transparency and control regarding the collection, use, and sharing of their personal information. The Alliance also supports clear and consistent rules that align with other privacy laws around the world and that support practical implementation and operationalization by news publishers of all sizes across digital and offline media, regardless of jurisdiction.

The Alliance, joined by the California Newspaper Publishers Association, respectfully submits the following comments on certain topics (designated below) as identified in the Agency's Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21) dated September 22, 2021.

I. Topic 1: Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses

The CPRA Regulations Should Align with Existing Privacy Laws, Including the GDPR, the VCDPA and the ColoPA.

Laws in Europe, and here in the U.S., have already outlined the circumstances in which a business' processing of personal information presents a "significant risk to consumers' privacy or security." As such, the Alliance recommends that the Regulations align with existing privacy laws on this issue, including the European Union General Data Protection Regulation ("GDPR")[3], the Virginia Consumer Data Protection Act ("VCDPA")[4], and the Colorado Privacy Act (ColoPA).[5] Such harmonization will provide much needed consistency and predictability as to when a covered business must perform cybersecurity audits and risk assessments with respect to their processing of personal information.

Under the GDPR, a Data Protection Impact Assessment ("DPIA") is only required where processing entails: (i) decisions based on automated processing, including profiling, that produce legal effects on natural persons; (ii) large scale processing of special categories of data or of data relating to criminal convictions; (iii) a systematic monitoring of publicly accessible data on a large scale; or (iv) activities publicly listed by the national supervisory authorities.

Similarly, under the VCDPA and the ColoPA, in order to present a significant risk to consumer's privacy, the profiling at issue must be made in furtherance of a decision by the controller that results in the provision or denial by the controller of: (i) financial and lending services, (ii) housing, (iii) insurance, (iv) education enrollment, (v) criminal justice, (vi) employment opportunities, (vii) health care services, or (viii) access to basic necessities, such as food and water (or, in the case of the ColoPA, access to "essential goods or services"[6]).

---

[3] GDPR Art. 35. *See also* "Guidelines on Data Protection Impact Assessment (DPIA)," available at https://ec.europa.eu/newsroom/article29/items/611236).

[4] Va. Code Ann. § 59.1-576.

[5] Colo. Rev. Stat. § 6-1-1301.

[6] Colo. Rev. Stat. § 6-1-1303(10).

The Alliance suggests that the Regulations should not require covered businesses under the CPRA to engage in the costly and burdensome task of submitting a risk assessment to the Agency unless the processing of personal information at issue rises to the level of "significant risk" identified in the GDPR, VCDPA, and ColoPA.

II. Topic 2: Automated Decisionmaking

The Rules Should Align with the GDPR and Should Appropriately Balance the Interests of Consumer Safety and Security with Those of Consumer Privacy.

The Agency is fortunate to be able to look to existing privacy law that describes the kinds of activities that should be deemed to constitute "automated decisionmaking technology" or "profiling." As such, the Alliance respectfully recommends that the Regulations should, wherever possible, align with the GDPR. Specifically, automated decisionmaking should be limited to decisions based *solely* on automated processing and which produce legal effects concerning a consumer or significantly affect a consumer in a similar way.[7]

Also consistent with the GDPR, the Regulations should allow for decisions based on automated processing or profiling (and limit a consumer's ability to opt out of such automated processing or profiling) where the processing is expressly authorized by law to which the business is subject, or necessary for entering into, or the performance of, a contract between the consumer and the business, and in situations where consumer safety could be endangered in the absence of such decisions (such as in the case of identity theft, and fraud monitoring and prevention).[8]

In addition, the Regulations regarding the kind of information businesses must provide to consumers in response to access requests, including what businesses must do in order to provide "meaningful information about the logic" involved in the automated decisionmaking process, should not require businesses to disclose trade secrets, confidential business information, or other information that might allow fraudsters or other bad actors making access requests to harm or jeopardize the security and safety of other consumers.

III. Topic 3: Audits Performed by the Agency

The Regulations Should Incorporate an Objective Standard for the Initiation of an Audit.

The Alliance respectfully recommends that the Regulations set forth an objective standard to guide the Agency's selection of which businesses it will audit and the Agency's determination of when an audit is necessary. In order to conserve scarce Agency resources, the Agency should initiate an audit when the Agency has evidence to support a reasonable belief that a violation of the CPRA has occurred. The scope of the audit should similarly be limited to the processing of personal information that gave rise to the purpose for initiating the audit. The Regulations should also include requirements for technical, administrative, and physical safeguards that the Agency must follow in order to protect consumers' personal information during the performance of the audit and to ensure that the audit is not unduly burdensome.

---

[7] GDPR Art. 22.

[8] GDPR Recital 71.

IV. Topic 4: Consumers' Right to Delete, Right to Correct, and Right to Know

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

The Alliance respectfully recommends that the Regulations modestly modify the CCPA regulations in order to address operational complexities raised by existing verification requirements. The CCPA Regulations currently provide as follows:

> Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request.[9]

The experience of businesses addressing complex and multifaceted verification requirements under the CCPA, and the time that consumers take to respond to such requests for verification, supports a slight revision of this aspect of the CCPA regulations. The time required for verification should not count towards the total time allotted for the business to complete the request. The Alliance therefore recommends that the Regulations revise the CCPA regulations such that the 45-day window to respond to requests to delete and requests to know begins to run on the day the request is verified by the consumer.

B. The Rules Should be Consistent with the Existing CCPA Regulations.

There are a number of processes and standards put in place under the CCPA regulations that should remain consistent under the CPRA Regulations. For example, under the CCPA regulations, businesses may offer the consumers the option to delete select portions of their personal information as long as a global option to delete all personal information collected from them is also offered and more prominently presented than the other choices.[10] The CCPA regulations also provide that "a business may use a two-step process for online requests to delete, where the consumer must first submit the request to delete and then separately confirm that they want their personal information deleted."[11] Further, the existing CCPA regulations specify that a business may comply with a consumer's request to delete their personal information by de-identifying or aggregating the information.[12] The CCPA regulations also provide that, if a "business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose."[13]

---

[9] 11 CCR § 999.313(b).

[10] 11 CCR § 999.313(d)(8).

[11] 11 CCR § 999.312(d)

[12] 11 CCR § 999.313(d)(2).

[13] *Id.* (d)(3)

The Alliance recommends that these existing CCPA regulations remain in place under the CPRA in order to provide consistent and predictable guidance to, and save unnecessary expense and burden for, businesses that have expended time and effort putting CCPA compliance programs in place.

V. Topic 5: Consumers' Right to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of Their Sensitive Personal Information

The Regulations Should Allow for Technologically Appropriate Approaches to Opt Outs Across Channels, and Provide a Grace Period for Organizations to Implement All Necessary Opt-Out Mechanisms.

Publishers value their trusted first-party relationships with their readers. Therefore, news media have worked tirelessly over the last two years to put in place consumer-friendly links and backend systems to allow consumers to opt out of sale, as that term is defined under the CCPA. The CCPA itself made clear that a Do Not Sell My Personal Information link, on websites and in mobile apps, was the method by which businesses were required to provide this choice to consumers. Due to legacy technologies and platforms that often vary across different publications, news media have faced tremendous challenges in implementing such opt outs across properties and geographies, not to mention addressing situations where sales may occur offline. It is already impossible, from a technological perspective, for one single link on a web page to meet all of these needs.

The CPRA affords consumers new rights to opt out of sharing for cross-context behavioral advertising and to limit the processing of their sensitive personal information. The explicit language of the CPRA helpfully provides businesses with a choice to either provide links for a consumer to exercise these rights or "allow[] consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, … to the business indicating the consumer's intent to opt out of the business' sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both."[14] The Alliance supports Regulations that mirror this language in the statute.

No single opt-out preference signal, including the Global Privacy Control, can provide a one-stop-shop for consumers to opt out of all sales and sharing for cross-context behavioral advertising, much less to limit the use of sensitive personal information. The Alliance respectfully submits that the Regulations should not mandate the use of the Global Privacy Control or any other single opt-out preference signal.[15] Instead, the Alliance recommends that the Regulations support the use of

---

[14] Civil Code § 1798.135(b).

[15] The Global Privacy Control is not an "Easy Button." It does not work on all browsers, much less mobile operating systems or offline. In the event that the Agency promulgates Regulations that mandate the implementation of the Global Privacy Control, it should also mandate that all browsers adopt the Global Privacy Control so that consumers are not misled that use of the Global Privacy Control can opt them out of all third party ad tracking on all browsers. In such an event, the Agency should also explicitly provide guidance on how businesses are expected to provide opt-out rights on mobile platforms and offline, where the Global Privacy Control is not supported.

the Global Privacy Control or another opt-out preference signal, but also allow businesses to put in place as many different technologically appropriate and conspicuous methods as needed to provide all consumers (regardless of their authentication status) with robust opt-out choices across all browsers, media, devices, operating systems, and platforms, as well as with respect to offline "sales" such as list rentals.

Further, given these new consumer rights and the challenges of implementing opt-out requirements in a manner that will be honored by downstream ad tech players (that publishers do not control), the Alliance also respectfully requests that the Agency incorporate a compliance grace period for such implementation, up to and including January 1, 2025.

VI. Topics 6 (Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information), and 8(b) (the Definition of "Sensitive Personal Information")

The Regulations Should Allow for First-Party Targeted Advertising Based on Reader Interest in Sensitive Content

The CPRA statute is clear that there are certain limited but critical circumstances in which consumers cannot opt out of processing of sensitive information: specifically, when such information is used: (i) to "improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business";[16] (ii) to "provid[e] analytic services"[17]; or (iii) for "[s]hort-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about a the consumer or otherwise alter an individual the consumer's experience outside the current interaction with the business."[18]

The Alliance respectfully requests that the Regulations align with the use cases described in the statute. In addition, the Alliance recommends that the Regulations support all forms of first-party advertising, even when such advertising is based on a reader's visit to an article regarding a sensitive topic. Publishers derive revenue (without which some outlets would not survive) by adding readers to aggregated demographic segments to which advertisements are targeted (such as "interested in medical articles"). Taking note of the fact that a consumer has read such an article does not equate with an inference that the reader has that sensitive condition at issue or is otherwise a member of group characterized by the sensitive condition. These segments are created based on whether a reader visited a particular article on a publisher's site regarding a sensitive topic. Such advertising is not based on the tracking of a device or an individual across sites or apps, and is limited to a single publisher's universe. Not only do many Alliance members heavily rely on such first-party advertising revenue but publishers also need the ability to use this first-party data (on a sensitive topic, or otherwise) to highlight or suggest similar content that the reader may be interested in (solely based on other articles the reader has viewed on the publisher's site). Without such an exception, medical news publications, for example, would not be able to use first-party data

[16] Civil Code § 1798.140(e)(8).

[17] *Id.* § 1798.140(e)(5).

[18] *Id.* §1798.140(e)(4).

to suggest other articles to a reader regarding similar symptoms or treatments. For both of these reasons, the Alliance recommends that the Regulations deem the use of information to create such segments for targeting as "collected or process[ed] without the purposes of inferring characteristics about a consumer" and therefore not subject to a consumer's right to limit use and disclosure of sensitive personal information. By contrast, the Alliance strongly supports Regulations that allow a consumer to limit the use of their sensitive personal information with respect to targeted advertising based on third-party tracking or sharing.

VII. Topic 7: Information to Be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)

The Regulations Should be Consistent with the CCPA Regulations, and Should Provide a Reasonable Standard For the Provision of Information Beyond a 12 Month Window.

For security reasons, the Alliance strongly supports the Regulations remaining consistent with those of the CCPA such that they prohibit disclosure of sensitive information in response to consumer's requests to know.[19] This is particularly relevant since the CPRA covers employee data, as employers necessarily store sensitive information of employees, including social security numbers, health and benefits information, and financial information.

In addition, the Regulations should adopt a reasonable standard to govern a business' determination as to whether providing information beyond a 12-month window would involve a disproportionate amount of effort. Certain data sets (for example, unstructured data) would require a disproportionate amount of effort even to piece together whether data belongs to a certain consumer; impossible should not be the standard.

VIII. Topic 8 Definitions and Categories

A. Topic 8(e): The Business Purposes for Which Businesses, Service Providers, and Contractors May Combine Consumers' Personal Information that was Obtained from Different Sources

Businesses and Their Service Providers and Contractors Should be Allowed to Combine Personal Information from Different Sources for Consumer-Friendly Business Purposes

Businesses and their service providers and contractors should be able to combine personal information from different sources for legitimate business purposes. Under the current CCPA regulations, a "service provider" cannot build or modify household or consumer profiles to use in providing services to another business, or correct or augment data acquired from another source.[20] The Alliance submits that the Regulations should support these uses of data by service providers in ways that promote consumer privacy, even if that involves the combination of information from different sources and/or the use of information to provide services to more than one business.

---

[19] 11 CCR § 999.313(c)(4).

[20] 11 CCR § 999.314(c).

For example, the Regulations should support the combination of personal information from different sources:

- To enable businesses to better understand the demographic make-up of the communities they serve, for internal business planning/benchmarking purposes. For example, publishers obtain age and gender data from a vendor to compile general statistics about the demographics of event attendees (but do not use this information to create profiles or individually target those attendees).

- For purposes of data hygiene. For example, publishers may use a vendor to check public databases to make sure the publisher has up to date, accurate contact information (name, mailing address, phone number) for their subscribers/users for direct marketing purposes. Section 999.314(c) of the CCPA regulations should be revised to allow for this practice as a business purpose, as it is both privacy- and consumer-friendly.

B. Topic 8(j): Defining "Dark Patterns" The Regulations Should Align with Existing EU Standards for Obtaining Consent.

The Alliance maintains that it is critical that the Regulations include clear parameters of what is an acceptable method to obtain consent or to provide choice to a consumer, where required (e.g., for financial incentive programs). Accordingly, the Regulations should align with existing guidance from EU regulators under the EU Privacy Directive that address the collection of consent for cookies and similar technologies. The Alliance would also welcome guidance in the Regulations as to examples of acceptable just-in-time notices for collecting such consent.

IX. Topic 9: Additional Comments The Regulations Should Give the Agency Flexibility in Enforcement with Respect to Employee and B2B Data.

The CPRA is intended to be a consumer privacy law, and that is what California voters acted on. Moreover, other states have consistently exempted information derived from or related to employees and business representatives from the scope of their consumer privacy laws, largely because that type of information is already rather heavily regulated. As such, the Alliance respectfully recommends that the Regulations allow the Agency to refrain from taking enforcement action for alleged violations involving employee information or information of business representatives. The Agency should not waste valuable time and limited resources on pursuing violations that distract from the Agency's priority of protecting consumer privacy.

X. Conclusion.

It has never been more clear that a vibrant and thriving free press cannot be taken for granted. To that end, the responsible use of digital advertising is critical to assuring that independent media do not cease to exist. Aligning digital data practices with consumer expectations can contribute to improving readers' trust in news at a time when it is under threat, and can help make the advertising market more competitive by decreasing the network effects caused by the consolidated and centralized data collection by third parties.

The Alliance looks forward to working with the Agency to craft forward-thinking Regulations that balance consumer privacy with the needs of independent journalism (which is so critical to a functioning democracy), and that could serve as a model for other states and jurisdictions around the world.

Sincerely,

Danielle Coffey
EVP & General
Counsel
News Media Alliance