August 23, 2022

regulations@cppa.ca.gov
California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

Re: Comments of the News Media Alliance in Response to the California Privacy Protection Agency's Notice of Proposed Rulemaking Issued with the Office of Administrative Law on July 8, 2022

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 in 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") is a nonprofit, non-stock corporation organized under the laws of the commonwealth of Virginia. It has no parent company. The Alliance represents news and media publishing associations, including nearly 2,000 diverse news and magazine publishers in the United States—from the largest nationally and internationally recognized organizations to hyperlocal news sources, from digital-only and digital-first to print news. Alliance members account for nearly 90% of the daily newspaper circulation in the United States. The Alliance is also the industry association for close to 100 magazine media companies with more than 500 individual magazine brands, that cover news, culture, sports, lifestyle, and virtually every other interest, vocation or pastime enjoyed by Americans. The Alliance diligently advocates for news organizations and magazine publishers on a broad range of issues that affect them today.

The Pew Research Center reported that, "the total combined print and digital circulation for locally focused U.S. daily newspapers in 2020 was 8.3 million for weekday (Monday-Friday) and 15.4 million for Sunday."[1] Digitally, in the fourth quarter of 2020, the top 50 newspapers saw almost 14 million unique visitors each month. In addition, there are on average more than 220 million magazine readers in the U.S. each year. Digital advertising is a significant source of revenue for these news and media outlets, large and small, and significantly helps keep the press (i) free from government control, (ii) affordable and accessible to all (not just to those who can afford a subscription), and (iii) at the highest level of integrity the people of the United States (and the world) have come to depend on. A thriving and free press has never been more important to American democracy. 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 and reliable news and media sources, while retaining control of the processing of their personal information.

The California Privacy Protection Agency (the "Agency") proposed regulations ("Regulations") promulgated pursuant to the California Privacy Rights Act ("CPRA"), which amended the California Consumer Privacy Act of 2018 (collectively with the CPRA, the "CCPA") and is effective January 1, 2023.

[1] See. "*Local Newspapers Fact Sheet*" by Katerina Eva Matsa and Kirsten Worden, available at https://www.pewresearch.org/journalism/fact-sheet.

The California Privacy Protection Agency Board (the "Board") approved the proposed Regulations and the Board filed a Notice of Proposed Rulemaking with the Office of Administrative Law on July 8, 2022. While the Regulations are helpful on a number of levels, they impose certain additional burdens on news and media organizations that will make compliance increasingly difficult, provide no added benefit to consumers, and fail to consider the implications of the employee and business relationship exemptions that expire January 1, 2023.

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 and that support practical implementation and operationalization by news publishers of all sizes across digital and offline media, regardless of jurisdiction.

The Alliance respectfully submits the following comments on certain topics (designated below) in response to the California Privacy Protection Agency's Notice of Proposed Rulemaking issued with the Office of Administrative Law on July 8, 2022.

I. The Agency Must Clarify the Scope of Protection for Journalism Set Forth in the CCPA.

The First Amendment to the U.S. Constitution and the California Constitution[2] protect a free and independent press. The text of the CPRA explicitly recognizes these constitutional protections by exempting those engaged in noncommercial journalism activities from the CCPA requirements:

> The rights afforded to consumers and the obligations imposed on any business under [the CCPA] shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article 1 of the California Constitution.[3]

The freedom of the press is protected under federal and state law, and should not be hindered by the inability of news and media outlets to engage in newsgathering activities or share information with those assisting in the creation and distribution of vital information to the people.

The Alliance asks the Agency (as within its power under the CCPA to establish "any exceptions necessary to comply with state or federal law"[4]) to make explicit in the Regulations that "selling" and "sharing" does not include conduct by those engaged in journalism or newsgathering, as those activities are inherently noncommercial. In other words, the Regulations should make clear that renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating (orally, in writing, or by electronic or other means), a consumer's personal information by a news media outlet to another business or to a third party in support of journalism is not "selling" or "sharing" under the CPRA provided that the

[2] California Constitution Art. I, §2.

[3] Cal. Civ. Code §1798.145(l). Section 2(b) of Article I of the California Constitution states as follows: "A publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication, or a by a press association or wire service, or any person who has been so connected or employed, shall not be adjudged in contempt by a judicial, legislative, or administrative body, or any other body having the power to issue subpoenas, for refusing to disclose the source of any information procured while so connected or employed for publication in a newspaper, magazine or other periodical publication, or for refusing to disclose any unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public."

[4] Cal. Civ. Code §1798.185(a)(3).

provisions of the CPRA are otherwise complied with (e.g., providing an accurate privacy policy and implementing reasonable security procedures and practices).

In addition, the Regulations should make explicit that, for purposes of fulfilling the intent of Section 1798.140(ag), all agreements between news media outlets and their vendors, even for purposes such as cross-contextual behavioral advertising, should be viewed as contracts with "service providers" for a "business purpose" and not subject to 11 CCR §7050(c),[5] provided that the vendor is otherwise prohibited from using that personal information other than as explicitly set forth in the agreement with the news media outlet, and not for any secondary purposes.

II. The Agency Should Provide Further Clarification on How to Properly Post Links Required under the CCPA and Regulations for Mobile Applications.

The Regulations provide that for mobile applications, links must be accessible within the mobile application.[6] The Regulations also require that the link to the privacy policy be on the platform page or download page of the mobile application,[7] the download or landing page of a mobile application,[8] and in the application's menu settings.[9] The notice at collection may be provided through a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.[10]

From an operational standpoint, these requirements are problematic because many mobile applications have limited space and mobile applications do not typically have footers, like many websites viewed on a mobile device. In addition, App Stores tend to place strict limitations on how, what, and where businesses can link to and from the mobile application's download page. 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 learn is an easily accessible location for important additional information.

Given these consumer expectations, and the fact that the Regulations dictate that all links required under the CCPA and Regulations be accessible via a privacy policy available to consumers on the mobile application download page,[11] the Alliance requests that the Agency clarify that if the required links are placed in the privacy policy and in the mobile application's hamburger menu or gearbox, they will be deemed "conspicuously placed" for purposes of the CCPA and the Regulations.

---

[5] 11 CCR §7050(c). "A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but those services shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or from its own interaction with consumers."

[6] 11 CCR §7003(d). "For mobile applications, a conspicuous link shall be accessible within the application, such as through the application's settings menu. It shall also be included in the business's privacy policy, which must be accessible through the mobile application's platform page or download page."

[7] *Id.*

[8] 11 CCR §7011(d).

[9] *Id.*

[10] 11 CCR §7012(c)(3).

[11] 11 CCR §7003(d).

Accordingly, the Alliance recommends the following revisions to 11 CCR §7003(d) to align with the language in 11 CCR §7003(c) and to clarify the placement of these links:

> For mobile applications, a conspicuous link required under the CCPA or these regulations shall be accessible within the application, such as through the application's settings menu~~. It shall also be included in,~~ and in the business's privacy policy, which must be accessible through the mobile application's ~~platform page or~~ download page.

All other references to the location of required links and notices with respect to mobile applications, including within the privacy policy, should either be removed or revised to align with the recommended language above. This will help provide uniformity across websites and among mobile applications such that consumers will know exactly where to look for privacy-related notices, no matter which format a consumer chooses to interact with the business.

III. The Agency Should Not Restrict a Service Provider's or Contractor's Ability to Use Information Collected from One Business for its Own 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. The Alliance submits that the Regulations should permit uses of personal information 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.

The Regulations provide:

> A service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except…[f]or internal use by the service provider or contractor to build or improve the quality of its services, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person.[12]

This provision would severely impact publishers' ability, for example, to use any service provider or contractor that provides analytic services to a publisher. Many technology service providers use a common data point (such as an IP address), received from multiple businesses, to provide services to many different businesses, to the benefit of consumers. For example, frequency capping or sequencing functions are extremely helpful to consumers because they limit the number of times consumers may see the same advertisement on a publisher's site. Service providers and contractors are only able to bring this benefit to consumers if they are able to take the information they receive from other similarly-situated businesses, and use that information collectively.

The Alliance recommends the following revision to 11 CCR §7050(b)(4):

> For internal use by the service provider or contractor to build or improve the quality of its services, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person unless the service provider or contractor is using the information solely for a business purpose that is disclosed in the business's privacy policy, to consumers when fulfilling a request to know, and in the contract with the service provider or contractor.

[12] 11 CCR §7050(b)(4).

IV. The Regulations Should Provide Further Guidance on the Requirements for Opt-out Preference Signals.

A. The Definition for "Frictionless Manner" Should Acknowledge Opt-Out Preference Signal Limitations.

The Regulations provide:

> In lieu of posting the "Do Not Sell or Share My Personal Information" link, a business may provide an alternative opt-out link in accordance with section 7015 or process opt-out preference signals in a frictionless manner in accordance with section 7025, subsections (f) and (g). The business must still post a notice of right to opt-out of sale/sharing in accordance with these regulations.[13]

However, what constitutes a "frictionless manner" under Section 7025(f) and (g) does not consider that opt-out preference signals, at least with their current technical capabilities, are virtually incapable of effectuating an opt-out in a "frictionless manner." It most certainly cannot be "frictionless" for traditional offline services, such as the content provided by print news and magazine publishers. Indeed, the very concept of the opt-out preference signal was to opt consumers out of cross-context behavioral advertising across browsers. 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. Meeting the Agency's definition of "frictionless manner" in online and offline contexts is impossible without forcing businesses to digitally combine all the information it could possibly have on a person, into a single database. It is hard to imagine that even the original drafter of the CCPA would want businesses to build massive databases, simply to meet the "frictionless manner" standard set forth in the Regulations.

Further, as the Regulations are currently drafted, providers of opt-out preference signals are not required to disclose these limitations to consumers, leading consumers to believe the opt-out preference signals can and will do more than is actually possible. Respectfully, it would be extremely harmful for consumers to be told opt-out preference signals are an easy one-stop fix, when in reality it is anything but that. The Agency should reconsider the definition of "frictional manner" to account for the technical limitations of opt-out preference signals. Considering the fact that additional methods to opt-out must be provided in a privacy policy and that notices of the right to opt-out have to be provided in the same manner in which the business collects personal information that it sells or shares (e.g., offline, through a connected TV, etc.),[14] the Alliance recommends the following revision to 11 CCR §7025(g)(3):

> Allows the opt-out preference signal to fully effectuate the consumer's request to opt-out of sale/sharing to the extent the business is able to effectuate the opt-out across browsers, devices, and offline databases based on the consumer information relayed to the business by the opt-out preference signal. For example, if the business sells or shares personal information offline and needs additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales or sharing of personal information, then the business has ~~not~~ fully effectuated the consumer's request to opt-out of sale/sharing to the extent it complies with the (i) opt-out preference

[13] 11 CCR §7013(d).

[14] 11 CCR §7013(e)(3).

signal for sales/sharing associated with the personal information provided to the business by the opt-out preference signal and (ii) with the other obligations set out in 7025(f) and (g).[15]

B. Providing Confirmation of Compliance with Opt-Out and Limit the Use Requests Should be Optional.

The Regulations provide:

> A business shall comply with a request to opt-out of sale/sharing by…[p]roviding a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business.[16]

The Alliance asks the Agency to recognize that this poses a significant burden on businesses without the technological, financial, and/or employee resources to build and properly effectuate compliance with this obligation. As such, the Alliance respectfully requests that the Agency make this optional until implementation is more feasible for businesses across the board.

V. Businesses Should Have 45 Days to Respond to a Request to Limit the Use of Sensitive Personal Information From the Date It Was Received.

The Regulations provide:

> A business shall comply with a request to limit by…[c]easing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (l) as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.[17]

For many businesses, the sale/sharing of personal information is limited to what is collected through various tracking technologies permitted to collect information from the website or mobile application. As such, a request to opt-out of the sale/share of personal information can be complied with by preventing the collection of information from those tracking technologies. The same cannot be said for the collection of sensitive personal information, simply by the nature through which sensitive personal information is received. Sensitive personal information is generally not collected by tracking technologies but manually inputted or uploaded by the consumer. As a result, complying with requests to limit the use and disclosure of sensitive personal information may take more human effort to effectuate versus a request to opt-out of the sale/share of personal information. This is true regardless of the fact that requests to limit do not need to be verified.

To address these operational complexities and to bring the consumer's right to limit sharing their sensitive personal information in line with the timeline for other consumer rights, the Alliance recommends that the Regulations provide businesses 45 calendar days to respond to a consumer's request to limit the use of sensitive information.

The Alliance recommends the following revision to 11 CCR §7027(g)(1):

---

[15] 11 CCR §7025(g)(3).

[16] 11 CCR §7026(f)(4).

[17] 11 CCR §7027(g)(1).

> A business shall comply with a request to limit by…[c]easing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (l) as soon as feasibly possible, but no later than ~~15~~45 ~~business~~ calendar days from the date the business receives the request.

VI. The Obligation to Notify Third Parties of Opt-Out and Deletion Requests Exceeds the Scope of the Agency's Rulemaking Authority and Should be Eliminated.

The Regulations provide:

> A business shall comply with a consumer's request to delete their personal information by…[n]otifying all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.[18]

and

> A business shall comply with a request to opt-out of sale/sharing by…[n]otifying all third parties to whom the business makes personal information available, including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises, that the consumer has made a request to opt-out of sale/sharing and directing them 1) to comply with the consumer's request and 2) to forward the request to any other person with whom the third party has disclosed or shared the personal information during that time period. In accordance with section 7052, subsection (a), those third parties and other persons shall no longer retain, use, or disclose the personal information unless they become a service provider or contractor that complies with the CCPA and these regulations.[19]

These proposed Regulations are problematic as they would require retroactive application of the do not sell and deletion obligations and thereby exceeds the scope of the Agency'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 and deletion obligations to apply retroactively. Moreover, the statute only requires a prospective obligation on businesses that honor do not sell requests.[20]

Second, businesses are not always in a position to push these obligations onto third parties. As the Agency is aware, often the biggest players within the ad tech ecosystem are unwilling to negotiate terms with other businesses. Even the most well-known companies, with actual bargaining power in most situations, are unable to negotiate contractual terms with vendors that comply with the CCPA and allow the businesses to flow down those obligations. Even where self-regulatory organizations have developed frameworks for compliance purposes, there is no guarantee that businesses can obligate third parties to comply for the same

---

[18] 11 CCR §7022(b)(3).

[19] 11 CCR §7026(f)(3).

[20] Cal. Civ. Code §1798.135(c)(4). "For consumers who exercise their right to opt-out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations."

reasons stated above. At the same time, these parties are still an essential and necessary part of the online ecosystem and the Alliance respectfully asks the Agency to acknowledge the positions taken by these essential vendors.

In order to avoid any retroactive application of the CCPA and to address the reality that businesses, especially small businesses, are almost never in a position to push obligations on third parties, the flow down obligation to third parties should be eliminated or a more practical approach should be adopted. For example, the Agency should require businesses to flow down the requests but not be responsible for the third party's compliance with those requests, regardless of whether it has actual knowledge that the third party is not complying with such requests, where the business was unable to negotiate more favorable terms.

VII. The Agency Should Increase the Number of Consumers that Would Trigger Metrics Reporting for Businesses.

The Agency has maintained explicit metrics reporting requirements for a business that "alone or in combination, buys, receives for the business's commercial purposes, sells, shares, or otherwise makes available for commercial purposes, the personal information of 10,000,000 or more consumers..."[21]

It is understandable that the Agency and consumers would benefit from such metrics reporting, particularly from businesses that process large amounts of data. However, the 10,000,000 consumer threshold is a low threshold in today's digital world and will trigger reporting requirements for many small and local publications who simply may not have the resources to fulfill this additional obligation.

The Alliance strongly recommends that the Agency consider increasing the consumer threshold that would trigger this metrics reporting obligation so that those reporting obligations truly apply to the businesses collecting large amounts of personal information. Accordingly, the Alliance believes that the "10,000,000 or more" consumer threshold should be increased to 40,000,000 or more consumers.

VIII. The Agency Should Enumerate Additional Business Purposes For Which Service Providers and Contractors Can Use Information It Collected On Behalf of a Business.

The Regulations enumerate certain uses for which a service provider or contractor may use personal information that it has collected on behalf of a business.[22] However, service providers and contractors need the flexibility to make other uses of such information for their own business purposes. For example, the Regulations only permit service providers and contractors to use such personal information "[f]or the specific business purpose(s) and service(s) set forth in the written contract required by the CCPA and these regulations" and "[f]or the purposes enumerated in Civil Code Section 1798.145, subdivisions (a)(1)-(4)."[23] This language would prohibit service providers and contractors from being able to create aggregated or de-identified data from such personal information (even where the agreement between the service provider or contractor and business specify the obligations for aggregated or de-identified data), and it is unclear to the Alliance why the Agency seeks to restrict such activity.

The language would also prohibit the building of consumer profiles to use in providing services to another business and the correction and augmentation of data acquired from another source in ways that promote consumer privacy.

---

[21] 11 CCR §7102(a).

[22] 11 CCR §7050(b)(1)-(6).

[23] *Id* at (b)(1)-(4).

The Alliance respectfully requests that the Agency consider enumerating the following business purposes in 11 CCR §7050(b): (i) the collection, use, retention, sale, and disclosure of consumer information that is deidentified or in the aggregate, (ii) 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); and (iii) the combination of personal information from different sources 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.

IX. The Agency Should Offer Guidance On How To Contractually Restrict Vendors Who Provide Services as a Third Party and as a Service Provider and/or Contractor.

The Regulations state that if a contract is for cross-context behavioral advertising the vendor cannot be a service provider.[24] However, often, technology providers offer a variety of services that could make them a service provider in one context and a third party in another, depending on the services being provided.

The Alliance asks the Agency to take this business reality into consideration and clarify in the Regulations that if the contract clearly sets out where the vendor acts as a third party for cross-contextual behavioral advertising, a service provider, and/or a contractor (and includes the necessary obligations for each, as appropriate) then the vendor should be deemed as acting in the role as set out in the agreement (provided that the vendor and business process personal information according to the terms and roles of the agreement, and otherwise comply with the CCPA).

X. The Agency Should Specify Regulations For Deceased Consumers.

As noted above, the CCPA defines a consumer as "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier."[25] The definition of "resident" in Section 17014 of Title 18 of the California Code of Regulations does not specify that the resident must be living.

Alliance members anticipate that households, family members, or estates, will attempt to use the consumer rights afforded in the CCPA to make requests on behalf of a decedent. The European Union's General Data Protection Regulation, for example, explicitly confirms that data subject rights do not apply to the personal data of deceased persons.[26] For the sake of transparency and consistency, the Alliance recommends the Agency make explicit that the CCPA applies only to living natural persons, consistent with other consumer-focused privacy laws.

---

[24] 11 CCR §7050(c). "A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising…A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor."

[25] Cal. Civ. Code §1798.140(i).

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Recital 27) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

XI. The Agency Should Restrict and Set Additional Obligations on Agency Conducted Audits.

The Regulations propose a broad audit right, with no restrictions or obligations whatsoever on the Agency in how it may conduct an audit. The scope of this audit right goes far beyond what is permitted by the CCPA. The Alliance respectfully submits that the Agency has failed to meet its obligation under the CCPA to issue "regulations to define the scope and process for the exercise of the agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena."[27] Pursuant to the CCPA, the Regulations should set forth an objective standard to guide the Agency's selection of which businesses it will audit, and clarify what constitutes a "significant privacy harm" that could give rise to an audit. Without a clear and objective standard, it will be difficult for businesses to sufficiently cooperate with an audit. Further, the Regulations do not appear to protect consumer personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena. The Regulations should 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.

The Regulations provide:

> [T]he Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law…Audits may be announced or unannounced as determined by the Agency.[28]

The Alliance requests that the Agency set more detailed boundaries before conducting an audit and to explicitly set out the procedures for which it must follow before conducting an audit. At a minimum, the Agency should specify with detail the steps the Agency shall take before conducting an unannounced audit and how the Agency should conduct itself during any audit it conducts. Further, the Agency should explicitly set out in the Regulations that the Agency is not permitted to conduct audits under the CCPA or these Regulations until the Agency has provided "guidance to businesses regarding their duties and responsibilities under [the CCPA] and appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with [the CCPA] pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185."[29]

XII. The Agency Should Remove Violations for Unintentional Dark Patterns

The Regulations provide:

> A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business's intent.[30]

In the Initial Statement of Reasons, the Agency takes the positon that because the use of dark patterns negates any agreement for consent, the use of dark patterns does not have to be intentional, it only needs to have "the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further

[27] Cal. Civ. Code §1798.185(a)(18).

[28] 11 CCR §7304(b) and (c).

[29] Cal. Civ. Code §1798.199.40(f).

[30] 11 CCR §7004(c).

defined by regulations."[31] However, a dark pattern should need to be designed or manipulated with such an effect, meaning that a truly unintentional dark pattern should not rise to a violation under the CCPA. Further, upon review of the annotated CPRA amendment, the annotation states that with respect to issuing regulations on the use of dark patterns to opt consumers back into the sale/share of personal information, there should be "No *coercive efforts* to dupe consumers into opting back into the sale of their information."[32] More importantly, with respect to the use of dark patterns negating consent, the annotation to this very provision of the CPRA states, "consumers cannot compete against unlimited computing power and *intentionally*-obfuscating terms & conditions, privacy policies, or *interfaces*." Clearly, the drafters of the CPRA amendment believed that the use of dark patterns involved some intention to subvert or impair user autonomy, decisionmaking, or choice on the part of the business.

Nevertheless, the Alliance recognizes that consent obtained through the use of a dark pattern, intentionally designed or not, should be invalid. However, the Alliance asks the Agency to consider that to the extent the business can show the use of the dark pattern was unintentional – for example, by proof that some internal process or review designed to remove dark pattern designs and manipulations was followed before implementation – such "unintentional" dark pattern will not amount to a violation of the CCPA if the business either (i) stops the processing of personal information for which the invalid consent was the basis of such processing; or (ii) obtains valid consent from the consumer to continue such processing.

XIII. The Agency Should Set Out Regulations Specifically for Employee Data and Business to Business Data

The Regulations do not consider the application of the CCPA or the Regulations to personal information and sensitive personal information collected in the employee or business to business (B2B) context (personal information that was previously exempt from most of the obligations in the CCPA).

The Alliance requests that the Agency, in accordance with its power under the CCPA,[33] draft Regulations that address how businesses should handle CCPA requests received from consumers in the employee or B2B context. For example, both employers and businesses operating in the B2B context process sensitive personal information in order to maintain and facilitate that relationship. The Regulations should explicitly carve out such uses from the obligation to offer the employee or the B2B consumer the right to limit the use of such sensitive personal information. Another example is the contents of a consumer's mail, email, and text messages, unless the business is the intended recipient of the communication. Often, the business is not the intended recipient of these communications but the communications are sent *for the benefit* of the business. Consumers acting in the context of the employee or B2B relationship should not be able to limit the use of such communications by the business for its own business purposes. Processing personal information collected by a business about a consumer, where the consumer is a job applicant, employee, owner, director, officer, medical staff member, or contractor of the business should be considered a "business purpose," to the extent that the business is processing the consumer's information within the context of those roles and relationship. Further, the processing of personal information reflected in a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company,

[31] Cal. Civ. Code §1798.140(l). "'Dark pattern' means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation."

[32] See. Annotation to Cal Civ. Code §1798.185(20)(C)(iii) (*emphasis added*); available at https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/.

[33] Cal. Civ. Code §1798.185(a)(19)(C)(i). "The Agency shall "issu[e] regulations, with the goal of strengthening consumer privacy while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer's sensitive personal information, including…determining any additional purposes for which a business may use or disclose a consumer's sensitive personal information."

partnership, sole proprietorship, nonprofit, or government agency *and* whose communications or transaction with the business occur within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency should also be considered a business purpose.

The lack of guidance regarding the treatment of personal information and sensitive personal information collected in the employee or B2B context, imposes a significant amount of uncertainty as well as meaningful compliance burdens on Alliance members. In addition to considering Regulations that address how businesses should handle CCPA requests received from consumers in the employee or B2B context, the Alliance also respectfully requests forbearance from enforcement of employee or B2B related violations to allow businesses to the necessary time to build and implement the necessary compliance policies and frameworks.

XIV. The Agency Should Delay Enforcement Until After Regulations Are Finalized

The Alliance recognizes that the Agency was given a tall order to meet the July 1, 2022 deadline and can understand the necessary but time-consuming steps it must take (and will continue to take) to draft and finalize these Regulations. The Alliance also recognizes the challenge with creating regulations that address privacy risk assessments, cybersecurity audits, and the use of automated decision-making.

That said, the Alliance asks the Agency to delay enforcement of these Regulations, given it has missed the July 1, 2022 deadline to adopt final regulations. News and media outlets subject to the CCPA need time to implement the Regulations once they are finalized. This will allow businesses, service providers, contractors, third parties, and in particular small publishers, the ability to take a reasonable amount of time to analyze and implement the Regulations. Alternatively, the Alliance respectfully requests that the Agency explicitly set out in the Regulations that the Agency shall not enforce against violations of the CPRA amendments if such violations occurred prior to July 1, 2023[34]; or against violations with respect to obligations only found in proposed regulations; or, with respect to automated decision-making, privacy risk assessments, and cybersecurity audits, until six months after such obligations are addressed in finalized Regulations.

XV. Conclusion

It has never been more clear that a vibrant and thriving free press cannot be taken for granted. To that end, removing onerous business obligations and imposing restrictions that would inhibit the responsible use of digital advertising are critical to assuring that independent media does not cease to exist. Further, aligning privacy practices with consumer expectations can contribute to improving readers' trust in news at a time when it is under threat.

[34] Cal. Civ. Code §1798.185(d). "Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended by this act shall remain in effect and shall be enforceable until the same provisions of this act become enforceable."

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.

Sincerely,

Danielle Coffey
EVP & General Counsel
News Media Alliance