MPA THE ASSOCIATION OF MAGAZINE MEDIA

Nov. 8, 2021

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

Re: Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)

Via email to regulations@cppa.ca.gov

Dear Ms. Castanon,

Thank you for the opportunity to comment on the Proposed Rulemaking by the California Privacy Protection Agency (CalPPA) on the California Privacy Rights Act of 2020's (CPRA) amendments to the California Privacy Protection Act of 2018 (CPPA). MPA – The Association of Magazine Media, the trade association for the magazine industry, represents over 500 magazine media brands that deliver high quality content to 90 percent of all U.S. adults through print and digital magazines. California is home to many of our members, who play an integral part of the state's economic fabric – by the end of 2019, the periodical publishing industry in California had supported 31,525 jobs and paid more than $844 million in annual employee wages.[1]

We recognize California's leadership on privacy and support attempts to balance consumer protection with workable provisions that recognize the operational and compliance challenges faced by many businesses.

Our comments below focus on five categories listed in the PNPRM that impact news and magazine media. They are: 1) Cybersecurity Audits and Risk Assessments Performed by Businesses; 2) Automated Decisionmaking; 3) Consumers' Right to Delete, Right to Correct, and Right to Know; 4) Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information; 5) Definitions and Categories.

1. Cybersecurity Audits and Risk Assessments Performed by Businesses

a. When a business's processing of personal information presents a "significant risk to consumers' privacy or security."

The CPRA requires businesses to perform a risk assessment, that is then documented for submission to CalPPA, with the goal of restricting or prohibiting processing of personal information if the risks to a consumer's privacy outweigh any benefits (to the consumer but also to the business, stakeholders and the public). Companies must also make a preliminary determination of data processing that may present a “significant risk” to the privacy of California residents.

To scope the agency’s efforts in this area, we suggest aligning the interpretation of “significant risk” with the General Data Protection Regulation’s (GDPR) concept of “legal effects concerning individuals” or the creation of “similarly significant” effect on individuals, which offers a useful standard for risk assessments that properly focuses the risk on actual or potential harm to individuals. As the UK’s Information Commissioner’s Office (ICO) and other data protection regulators have, we suggest that CalPPA offer guidance on the type of conditions that must be met for processing to be considered a “significant risk” to a person’s privacy or security as well as potential ways to modify processing to mitigate this risk.

Additionally, covered businesses should be required to perform risk assessment only when the processing of personal information rises to the level of “significant risk” as identified in the GDPR (as well as the Virginia Data Protection Act (VCDPA) and the Colorado Privacy Act (ColoPA)). Finally, we believe risk assessments should only be required for each materially different type of processing involving sensitive personal data or new profiling that includes sensitive personal data and the agency should publish a standard risk assessment form.

b. When “the risks to the privacy of the consumer [would] outweigh the benefits” of businesses’ processing consumer information, and when processing that presents a significant risk to consumers’ privacy or security should be restricted or prohibited.

Determining the ratio of risk to benefit is already a challenging task for companies but it becomes almost impossible without a standardized understanding of both “risk” and “benefit,” as well as a commonly accepted way for commercial entities to determine the monetary value of personal information. We agree with the concept of measuring risk and benefit against the complexity of data processing and the sensitivity of the information, with prohibitions graded against risks (such as bodily harm, freedom, discrimination, identity fraud, etc.) but advise the agency against a broad rulemaking that goes beyond its purview in this case. The CCPA, as amended by the CPRA, does not restrict or prohibit processing of personal information; instead, it grants consumers rights to receive notice and clear choices regarding the sharing of their information in certain limited circumstances. Therefore, it's not clear whether the agency’s authority under CPRA would empower it to create new restrictions and prohibitions on the processing of personal information based on a new risk/benefit calculus. To better understand the risks and benefits of processing personal information, and potentially develop a standardized approach, we
propose the agency convene a workshop with key stakeholders with the aim of producing a usable risk/benefit rubric that could be adopted by covered entities.

2. Automated Decisionmaking

a. What activities should be deemed to constitute “automated decisionmaking technology” and/or “profiling.”

To determine the scope of activities that should constitute automated decisionmaking or profiling, we suggest the agency look to the definition put forth by the ICO, which states “Automated decisionmaking is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data." Provisions on automated processing in the ColoPA and VCDPA, which allow individuals to opt-out of consequential AI-driven profiling and decisionmaking, might also be a useful reference (CO § 6-1-1306(a)(I)(C); VA § 59.1-573(A)(5)) as might work being done by the National Institute of Standards and Technology (NIST) to develop a voluntary AI Risk Management Framework.

Consistent with the statutory plain language, as well as the ICO's definition, we support rules that apply to truly, fully automated decisionmaking, not general human use of a computerized process to aid in a human decision. We caution against overly broad regulation of widely adopted and accepted categories of technology that would impede the use of socially beneficial and low-risk tools, to the significant detriment of both California consumers and businesses. Without reasonable limitations in place, any requirements established in this proceeding would substantially regulate a host of business activities that rely on some degree of automation for efficiency but are not AI. In these cases, human review intervenes and can explain, respond to complaints, and mitigate risk of arbitrary or inaccurate decisions.

We also request more information on how businesses can meet consumer expectations for privacy and security, as they related to automated processing, in different contexts, such as those delineated by the CPRA in relation to profiling ("...decisions related to a consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or real-time movements.")

b. What information must businesses provide to consumers in response to access requests in order to provide "meaningful information about the logic" involved in the automated decisionmaking process?

The CPRA and other privacy laws aim to provide consumers with more transparency and actionable insight into how their personal information is used in automated decisionmaking. But it's not clear how to define or deliver "meaningful information about the logic." "Meaningful information" is a subjective phrase, and we urge the agency to adopt flexibility in its interpretation of these provisions, as they represent an unsettled, and constantly evolving, area of data science, law and policy. Broadly, "meaningful information" should be relevant, both personal and contextual, and empowering – in other words, information that is contextual, personal, and actionable that allows an individual to make informed choices about if and how they want their data to be used.2

Existing resources may be useful as the agency considers the contours of notice for AI-driven processing, such as a report from the ICO and The Alan Turig Institute which offers a list of general types of explanation, including explaining the "rationale" that led to a decision and detailing the steps in the design of the AI to ensure "fairness."

3. Consumers' Right to Delete, Right to Correct, and Right to Know

a. The new rules and procedures, or changes to existing rules and procedures, needed for consumers to make requests to correct inaccurate personal information.

We urge CalPPA to ensure the rules related to individual rights are consistent with both the CCPA and GDPR since many companies have already implemented processes for these provisions. The rules should treat consumer correction requests similarly to access or deletion requests for "specific pieces of personal information," thereby excluding the correction of personal data elements that are exempt from both access and deletion requests under the Attorney General's CCPA Rules. Moreover, consistency on these rules will support companies that have already implemented consumer data correction protocols as part of their business practices (Colorado and Virginia will require doing this in 2023).

In addition, the agency should provide guidance on the "commercially reasonable efforts" standard related to individual rights to illuminate practices that qualify as reasonable. This standard could also be applied to documentation used to authenticate the accuracy of consumer information, since the process for determining whether this information is inaccurate is unclear.

4. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information

> ***a. What requirements and technical specifications should define an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information.***

MPA supports the ability of consumers to use an opt-out signal, and many of our members honor the Global Privacy Control (GPC) and other opt-out signals, but we ask for clarity on the provisions in the CCPA and CPRA, which we believe have conflicting language. The CCPA requires providing opt-out tools that offer users sharing options and that are free of defaults that might constrain or otherwise presuppose an individual's intent. The CPRA, on the other hand, endorses honoring a privacy control like the GPC. But the GPC, as currently designed, is a user signal that lacks granular sharing options and that is increasingly on by default in popular web browsers. In addition, CCPA regulations require covered entities to honor user-enabled privacy controls while the CPRA characterizes these controls as just one option for businesses complying with the opt-out. CalPPA should clarify this language to ensure compliance consistency.

We also ask the agency to continue defining the contours of a global opt-out signal, with stakeholder input, rather than mandating the use of the GPC or other specific opt-out tool. This will provide publishers with some flexibility to try different technical approaches across platforms, devices, and authentication statuses. On authentication, in particular, it's not clear how companies honoring the GPC, or other opt-out, should enact a user's preferences without knowing their identity. We do not believe the regulations intend for businesses that do not have direct identifiers to use probabilistic matching (which can be inaccurate) or combine offline and online data to comply with a privacy request. CalPPA should clarify that businesses do not have an obligation to associate online identifiers with offline data nor try to link devices unless it already does so through a consumer account as part of existing business practices.

5. Definitions and Categories

> ***a. Updates or additions, if any, that should be made to the categories of "sensitive personal information" given in the law.***

The CPRA gives consumers the right to request that a business limit the use and disclosure of their "sensitive personal information," but businesses need not honor such requests where the information is used: (1) to "improve, upgrade, or enhance the service or device that is owned, manufactured,

manufactured for, or controlled by the business"; to "provid[e] analytic services"; or for "[s]hort-term, transient use, including, but not limited to, non-personalized 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." The statute also limits honoring an opt-out when information is "collected or processed without the purpose of inferring characteristics about a consumer."

Many publishers rely on knowing the content that visitors engage with, including topics that might be considered sensitive, to highlight or suggest similar content or deliver advertising based on aggregated demographic segments. These segments are created based on the type of content a person reads or views and not on tracking them or their device(s) across other sites or apps. Content recommendations and advertising like this, which are fundamental to revenue-generation for news and magazine publishers, are contemporaneous to a person's interactions with a publisher and remain exclusively within the first party publisher context, and align with a consumer's expectations as they browse or otherwise engage with content. For these reasons, the agency should consider this type of information to be "collected or processed without the purpose of inferring characteristics about a consumer" and these activities (publisher collection and use of content-related information for the purposes of recommending or highlighting content, creating aggregated segments, and delivering targeted advertising) to meet the definition of "short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer's interaction with the business …[etc]" and therefore not subject to a person's right the limit use and disclosure of sensitive personal information. CalPPA must also ensure that the delivery of content recommendations and segment-based advertising based on the type of content a person reads or views is excluded from the concept and/or definition of "inferring characteristics."

b. Further defining the business purposes for which businesses, service providers, and contractors may combine consumers' personal information that was obtained from different sources.

Combining consumer personal information from various sources, such as third parties, to deliver tailored marketing campaigns and targeted advertising, is considered a "business purpose" under the CCPA. We request clarity on whether "service providers," as defined by the law, may have independent, direct relationships with a consumer at the same time, and whether they are then permitted to combine the consumers' personal information from different sources, such as third parties, to fulfill their business purposes. While we support reasonable limits on the practice of combining data, we also believe that individuals should be able to continue to receive the services that they would normally expect with different entities. For example, a consumer might visit a favorite publisher's site, using Google's login feature to access their account. But the relationship with Google, from a consumer expectation standpoint, ends there. Providing access to their account does not mean the consumer is consenting to Google to collect and/or combine any of their personal information.

We endorse limitations on data combining in circumstances when it is:

- Aligned with a consumer's expectations (an expected as part of the consumer's relationship with the service provider).

- Consistent with risk, fraud, and security and integrity requirements in the CPRA.
- Consistent with the consent of the consumer.

Finally, we urge the agency to consider that consent "fatigue" is real. If consumers begin to expect to have to opt in to simply use the service, or face a flurry of notices, they are likely to devalue the notices and less likely to make a distinction between reasonable and harmful uses of data.

c. The regulations, if any, that should be adopted to further define "dark patterns."

Establishing and maintaining trusted relationships with our audiences is a top priority for news and magazine media, and that starts by communicating, in language and visuals, with users in a direct and transparent way. The CCPA gives consumers the right to prevent advertisers from using processes intended to impair a consumer's choice to opt out, while the CPRA defines a dark pattern as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation" and makes clear that "agreement[s] obtained through use of dark patterns does not constitute consent." Colorado, Connecticut and Washington have all introduced privacy legislation that uses the same definition of dark patterns while the Federal Trade Commission has indicated it will issue more guidance on this. We support the agency's work in protecting consumers against entities who intentionally design elements to trick or manipulate individuals and ask for detailed guidance from CalPPA on what exactly they consider to be dark patterns, with visuals that showcase different contexts and designs that are problematic and approaches that avoid these problems.

Because of the complexity of regulating this issue, the agency might also review existing guidance, such as the Federal Trade Commission's "DotCom Disclosures" on digital advertising, and to approve self-regulatory schemes such as the Better Business Bureau's National Advertisers Division (NAD), which monitors advertising for truth and transparency, is another option as the watchdog's criteria for ads would include most, if not all, dark patterns. NAD considers whether advertising meets one or more criteria that include whether the ad is targeting a vulnerable population, capitalizing on consumer fears or misunderstanding, and/or concerns claims that consumers cannot evaluate for themselves. Having the force of law behind these programs, via CalPPA, provides the necessary accountability while avoiding the duplication of efforts.

MPA supports clear and consistent rules that align with other privacy laws around the world and that support practical implementation and operationalization by magazine media and publishers of all sizes across digital and offline media, regardless of jurisdiction, lessening the heavy compliance burden that would fall upon news and magazine media companies. Earning the trust of our readers and upholding consumer privacy is an extremely high priority for media and journalism entities and we welcome the opportunity to engage with you on these issues.

Sincerely,

Michelle De Mooy
Senior Director of Policy

Rita Cohen

Rita Cohen
Senior Vice President, Legislative and Regulatory Policy