
From: Blake Edwards [REDACTED]
Sent: 11/8/2021 11:00:23 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Stuart Pardau [REDACTED]; Howard Fienberg [REDACTED]
Subject: PRO 01-21 — Comments of the Insights Association
Attachments: Insights -- CPRA Comments. 11.8.21.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Please see attached. And thank you for the opportunity to comment.

—

Blake M. Edwards
Law Offices of Stuart L. Pardau & Associates
12121 Wilshire Blvd, Suite 805
Los Angeles, CA 90025
p: [REDACTED]
e: [REDACTED]



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

November 8, 2021

Re: Comments of the Insights Association on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)

Ms. Castanon:

The Insights Association (“Insights”) submits the following comments regarding future regulations relating to the California Privacy Rights Act of 2020 (“CPRA”).

Representing more than 750 individuals and companies in California and more than 6,000 across the United States, Insights is the leading nonprofit trade association for the market research¹ and data analytics industry. We are the world’s leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations, employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

The CPRA is going to have a profound impact on the business community, including the market research and data analytics industry. Small and medium-sized research firms in particular will face tremendous costs in updating and expanding on their already-extensive compliance efforts in connection with the California Consumer Privacy Act of 2018 (“CCPA”). Accordingly, and on behalf of our members, we commend your decision to seek input on future regulations and are grateful for the opportunity to comment.

1. Limit processing which presents a “significant risk” to consumers’ privacy or security to highly sensitive personal information, such as financial account information

The CPRA directs the Agency to issue regulations “requiring businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy” to perform annual cybersecurity audits and submit regular risk assessments to the Agency. The Agency has specifically requested feedback on this provision.

¹ Market research, as defined in model federal privacy legislation from Privacy for America, is “the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (ii) used to advertise or market to any particular individual or device.” See Part I, Section 1, R: <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/>

We respectfully request that processing which presents a “significant risk” be limited to processing of highly sensitive personal information, such as financial account or payment card information, social security numbers, or other personal information which, if breached, could result in immediate financial harm to consumers.

2. Limit processing which presents a “significant risk” to processing which occurs on a regular basis or a minimum number of times per year

In addition to limiting “significant risk” scenarios as described above, the Agency could also clarify that such processing must occur on a regular basis, or at least with some minimal frequency, to trigger the auditing and risk assessment requirements. It does not meaningfully further the spirit of the CPRA, and imposes particularly unnecessary burdens on small businesses, to require an audit and security assessment solely on the basis of one, two, or a handful of isolated instances of processing deemed to present a “significant risk” in a given year.

3. Limit processing which presents a “significant risk” to processing of at least 100,000 records

Alternatively, we suggest the Agency could incorporate some numerical trigger into what constitutes “significant risk” processing. For example, this number could track the figure in the CPRA’s “business” definition of 100,000 records, or the Agency could select some lower number. In any case, the underlying statutory language of the CPRA counsels in favor of some such numerical limit. The statute contemplates “significant risk to consumers’ privacy or security,” language which connotes larger concerns of aggregate risk, not every isolated presentation of risk to any individual consumer or small group of consumers.

4. Limit the audit and risk assessment requirement to businesses who meet one of the first two prongs of the CPRA’s “business” definition

As the Agency is aware, there are three different ways for an organization to be defined as a “business” under the CPRA: (1) annual gross revenues in excess of \$25 million; (2) buying, selling, or sharing the personal information of at least 100,000 consumers or households; or (3) deriving 50 percent or more of its annual revenues from selling or sharing personal information.

Because the third prong is not tied in any way to business size or processing volume, it includes a substantial number of small and medium-sized firms in the market research and data analytics industry. Firms who are subject to CPRA solely on the basis of this third prong should be exempt from any annual audit and risk assessment requirements. These audits and risk assessments will be time consuming and expensive, and could in fact cripple small businesses who are just trying to do legitimate marketing research and data analytics work which benefits larger businesses, nonprofit and educational organizations, government entities, and individual consumers.

Alternatively, the Agency could limit the audit and assessment requirements based on smaller limits than those in the CPRA’s “business” definition (e.g., firms that do \$15 million in revenue or deal with at least 50,000 records), to protect the smallest businesses from overly onerous regulatory requirements.

5. Clarify that use in research results and reports of “sensitive personal information” is a “reasonably expected” use of information provided in connection with corresponding surveys and research studies

Under the CPRA, consumers have the right to request that a business “limit its use of the consumer’s sensitive personal information to that use which is necessary to perform the services or provide the goods

reasonably expected by an average consumer who requests such goods or services.” The Agency has specifically requested comment on “what use or disclosure of a consumer’s sensitive personal information by businesses should be permissible notwithstanding the consumer’s direction to limit the use or disclosure of the consumer’s sensitive personal information.”

Insights is concerned that if research subjects who have provided sensitive personal information in connection with a survey or study (for example, in connection with a poll about an important political issue) submit such a request, this may compromise research results and leave market research firms in a legally unclear relationship with the research subject. Accordingly, the regulations should stipulate that use of sensitive personal information in research results, and the continued use of those results to draw insights about consumers, is a “reasonably expected” use of sensitive personal information which was freely provided in connection with a survey or research study.

6. Define “disproportionate effort” as those efforts which “do not, in the reasonable discretion of the business, meaningfully add to the consumer’s understanding of the business’s historical practices”

The CPRA preserves a consumer’s right to “know” what personal information is being collected and what personal information is sold or shared and to whom. Previously, under CCPA, these rights were limited to a 12-month “look-back” period. Under the CPRA, if a consumer requests to know how information has been collected, sold, or shared, no matter how far back that request might reach, the only limitation on the request is whether it would be “impossible, or involve a disproportionate effort” on the part of the business.

The Agency has specifically requested input on what standard should govern a business’s determination that providing information beyond the 12-month window is “impossible” or “would involve a disproportionate effort.” In the market research and data analytics industry, information relating to a particular research subject (especially if that research subject participates in a research panel, for example) may appear in multiple studies across a long period of time. A research firm could spend theoretically limitless time and resources to reconstruct all the times a research subject was involved in a study, what information that study collected, and with whom the results were shared. Reconstructing every such instance would not meaningfully advance the consumer’s rights under CPRA, and it is not clear how much of this “reconstruction” would constitute “disproportionate effort.”

Accordingly, the Agency should clarify that “disproportionate efforts” beyond the 12-month window are “those additional efforts which require time and expense on the part of the business, but do not, in the reasonable discretion of the business, meaningfully add to the consumer’s understanding of the business’s historical practices.” In the above-referenced panel participant scenario, for example, rather than reconstructing the facts around every past study, the business would only be required to make the requested disclosures beyond the 12-month window as necessary to ensure the research subject has a complete (if not completely granular) view of how the research subject’s information is being processed.

7. Exempt market research from notices of financial incentives

For our members’ research to be effective, they must ensure robust participation. This is frequently done through offering financial incentives. For example, a doctor may be offered an honorarium to answer a survey about various pharmaceuticals, or an individual may be offered a gift card to participate in a half-day focus group about the latest television shows.

Our industry has worked hard to comply with the financial incentive notice requirement under CCPA, but the notice of financial incentives requirements were not written with market research in mind; they inhibit research in an unintended way. Accordingly, we resubmit our request, made previously in connection

with the CCPA regulations, that market research incentives and similar rewards to research subjects be exempt from notices of financial incentives requirements under the CPRA. Most significant of all, appropriate notices of financial incentives are already provided in every legitimate market research execution. Adding parallel and/or potentially conflicting requirements will only confuse the issue for Insights members, their clients and the public at-large that participates in this research.

8. Limit the “authorized agent” concept to minors, and elderly or incapacitated individuals

Under the CPRA, a consumer may designate an authorized agent to submit opt-out requests, and requests to know and delete. There is currently no limitation on this procedure. Anyone can submit a request through an authorized agent. Increasingly, our members are receiving requests from purported authorized agents and are caught between, on one hand, wanting to honor legitimate requests and, on the other, the pervasive concern that the authorized agent mechanism invites fraud. Of course, our members take steps to verify such requests, as required by law, but those verification efforts are sometimes difficult to complete without requesting additional information, and tend to frustrate agents and/or consumers as much as they frustrate the business.

The registered agent option is unnecessary in the vast majority of cases, increases paperwork associated with the verification process, and opens the door for fraudulent requests designed to harm consumers. Except in cases where the consumer is a minor, or someone who genuinely needs an authorized agent to submit a request (such as an elderly or incapacitated individual), the purpose of the law is better served by requiring requests to be submitted by consumers themselves.

We hope the above comments will be useful to you and your team, and we are happy to entertain any questions or concerns you may have about the market research and data analytics industry.

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

Stuart Pardau
Counsel to Insights Association

Blake Edwards
Counsel to Insights Association

From: Matthew Schwartz [REDACTED]
Sent: 11/8/2021 11:03:45 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 - App Association Comments
Attachments: act_
_the_app_association_comments_on_proposed_rulemaking_under_the_california_privacy_rights_act_of_2020_FINAL.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Good morning,

Attached, please find comments from ACT | The App Association in response to the Agency's Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020. Please do not hesitate to reach out if you have any follow-up questions regarding our comments or if we can be of any help as you continue to move through the rulemaking process.

Best,

Matt Schwartz
Privacy Fellowship Coordinator
ACT | The App Association
[REDACTED]

November 8, 2021

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

RE: ACT | The App Association Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020

I. Introduction and Statement of Interest

ACT | The App Association (App Association) appreciates the opportunity to submit comments in response to the California Privacy Protection Agency's (CPPA or Agency) invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA). In general, the App Association supports the Agency's rulemaking efforts insofar that they ensure a clear and fair set of rules for both small businesses, like our member companies, and consumers. It is vital that the Agency strike an appropriate balance between honoring the spirit and intention expressed in the underlying statute, while at the same time ensuring those efforts do not pose unnecessary burdens to businesses or inhibit the growth and prosperity of California's innovation ecosystem.

The App Association represents thousands of small business software application development companies and technology firms, including many based either in California or conducting business in California and meeting one of the statutory thresholds designated in the law. Our member companies create technologies that generate internet of things (IoT) use cases across consumer and enterprise contexts and are primary drivers of the global digital economy. Today the ecosystem the App Association represents—which we call the app economy—is valued at approximately \$1.7 trillion and is responsible for tens of millions of jobs around the world, including 702,010 in California alone.¹ Alongside the world's rapid embrace of mobile technology, our members provide innovative solutions that power IoT, a market projected to be worth more than \$18.5 trillion by 2022 across modalities and segments of the economy.²

¹See *State of the U.S. App Economy: 2020*, ACT | THE APP ASSOCIATION, (2020) available at: <https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf> (noting that California has an estimated 702,010 App Economy workers as of 2020).

² Michael Luciano, *Global IoT Market Value Could Exceed \$14 Trillion*, ECN, (April 16, 2018) available at: <https://www.ecnmag.com/blog/2018/04/infographic-global-iot-market-value-could-exceed-14-trillion>

Consumers who rely on our members' products and services expect that our members will keep their valuable data safe and secure. The small business developer community the App Association represents practices responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations, and as such, ensuring that the company's business practices reflect those expectations by utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity.

The App Association serves as a leading resource in the privacy space for thought leadership and education for the global small business technology developer community.³ We regularly work to keep our members up to speed on the latest policy and legal developments and to translate those into practical and useable guidance, including on California privacy law, to ease the burden of compliance.⁴

II. General Comments

The App Association welcomes the CCPA as it prepares its first foray into regulating California's privacy space as authorized through CPRA. The CCPA assumes an immensely important role as the nation's only state-specific data protection agency in a state with the largest economy in the nation, the 5th largest economy in the world if taken on its own, and the largest app economy workforce of any state. Furthermore, as many have pointed out, CPRA is an incredibly ambitious and densely drafted law, uniquely so compared to other existing comprehensive state privacy laws and proposals. As such, interpreting and extending the law in accordance with the law's text and the drafter's intentions will require great solicitude from the Agency.

Despite its length and prescriptiveness, the law as approved creates many areas of lingering ambiguity, some intentional, some not, and some expressly subject to further rulemaking. With this invitation for comment, the Agency considers several of those important topics specifically earmarked for future proposed rulemakings, including cybersecurity audits, automated decision making, Agency compliance audits, guidelines on the right to correct inaccurate information, guidelines on the right to opt out of processing, guidelines on the right to limit disclosure of sensitive information, guidelines

³ See e.g., ACT | The App Association, *Innovators Network Foundation Announces Inaugural Privacy Fellows* (September 2019), available at: <https://actonline.org/2019/09/23/innovators-network-foundation-announces-inaugural-privacy-fellows/>.

⁴ See e.g., ACT | The App Association, *General Data Protection Regulation Guide* (May 2018), available at: https://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf; *What is the California Consumer Privacy Act (January 2020)*, available at: <https://actonline.org/wp-content/uploads/What-is-CCPA.pdf>.

on the right to know, and updates to definitions of key terms within the law. The final rules are due by July 1, 2022, and, clearly, this marks the beginning of a complex process that will likely require the Agency to undertake several rounds of deliberation to fully complete.

In the view of the App Association, the Agency should adopt a risk-based approach to its authority by prioritizing rules and enforcement actions that mitigate the most harmful activities that exist *today* and that erode consumer trust digital marketplace on a widespread basis. For example, the Agency should first rectify existing instances of non-compliance among the largest, data-hungry digital companies, such as through the evasion of the definition of sale under the law for the purpose of continuing a surveillance-based targeted advertising business model.

Other good examples of harmful practices to take aim at are those enjoined by recent settlements reached by the Federal Trade Commission (FTC). For example, the FTC recently reached a settlement with Flo, a popular fertility and period tracking app that allegedly shared the “health information of users with outside data analytics providers after promising that such information would be kept private.”⁵ The healthcare innovations our member companies produce—from heart condition detection to chronic condition monitoring to simply managing digital health information across health systems—are far too important for us to let them fall victim to foundering consumer trust in digital health earned by bad actors.

Under CPRA, the Agency enjoys fairly substantial latitude in deciding what rulemakings to pursue. The law enumerates 22 specific areas eligible for future rulemakings while also allowing the Agency to pursue any other rulemakings that “further the purposes of this title.”⁶ Uncertainty regarding which of the many potential areas of regulation the Agency seeks to pursue is suboptimal, especially for smaller businesses who may need longer lead times to update their compliance programs as further guidance from the Agency emerges. Going forward, the Agency should make a diligent effort to clearly telegraph which of its regulatory authorities it seeks to flex so that both consumers and the marketplace receive as much advance notice as possible.

The App Association also urges the CPPA to consider how forthcoming regulation can be scaled such that compliance requirements reflect the risk of activities posed by the regulated entity. Often, comprehensive privacy legislation and regulations are written with the intention of curbing the bad practices of some of the largest and most complex

⁵ Press release, “Developer of Popular Women’s Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data,” Fed. Trade Comm’n (Jan. 13, 2021), available at <https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc>.

⁶See California Civil Code §1798.185 (a), as amended in CPRA through §1798.185 22(d)

entities in the digital space. While this is often a worthwhile goal, if compliance requirements meant for larger entities apply equally across the digital ecosystem, the resulting burden may disproportionately harm smaller entities with less sophisticated and extensive compliance departments. Such regulatory arbitrage might ultimately prove counterproductive, reducing competition and innovation along the way.

III. Comments on Specific Topics for Proposed Regulation

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

CPRA permits the Agency to issue regulations “requiring businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security” to “perform a cybersecurity audit on an annual basis” and submit to the Agency regular risk assessments regarding their processing of personal information.⁷ The risk assessment requirement is consistent with existing regulatory structures, such as in the European General Data Protection Regulation (GDPR) and in other existing state privacy laws in Virginia and Colorado. As such, the App Association urges the Agency to harmonize its requirements with those already in place in those jurisdictions, such as by instituting similar requirements for businesses to conduct a risk-benefit analysis that weighs the benefits of their processing against the potential risks to the rights of the consumer associated with such processing. Similarly, the Agency could look to those jurisdictions in determining what processing activities present “significant” risk to consumers’ privacy or security. For example, the Agency could use as a guidepost Colorado’s “heightened risk of harm” standard, which includes any business that sells personal information or processes sensitive information.⁸

On the other hand, a cybersecurity audit requirement would be unique to California and could potentially unnecessarily burden smaller businesses without yielding commensurate benefits to consumer data security. The App Association believes any cybersecurity audit requirements should only apply to businesses with complex data processing operations or that process sensitive consumer information on a regular basis. While we do not advocate for a threshold based on firm-size alone, we urge the Agency to take into account the complexity of the processing detailed in the business’s data risk assessments before mandating a separate cybersecurity audit framework for smaller businesses.

Automated Decisionmaking

⁷ See California Civil Code §1798.185(a)(15)

⁸ See Colorado Revised Statutes §6-1-1309

CPRA authorizes CPPA to issue “regulations governing access and opt-out rights with respect to businesses’ use of automated decisionmaking technology, including profiling” and to require businesses to provide information about the logic underlying those decisions.⁹ Again, this new right comports with newly introduced frameworks in other jurisdictions, including Virginia and Colorado. We urge the CPPA to harmonize its forthcoming regulations with those laws. For example, Virginia and Colorado currently employ identical definitions of the term “profiling” and adopt the 45-calendar day deadline for responding to consumer requests that also exists in CPRA for other consumer rights.

Agency Audits

CPRA grants the CPPA audit authority over covered business’ compliance with any section of the law. As stated in our general comments, the Agency should focus its oversight authority on the companies with the most power to harm consumers on a widespread basis and to undermine trust in digital products and services.

Consumers’ Right to Correct

CPRA expanded on CCPA’s slate of consumer rights (the right to delete data, the right to know what data is collected, the right to access data, and the right to know what data is shared or sold) by adding a new right to correct inaccurate personal data. Businesses are instructed to use “commercially reasonable” efforts to correct inaccurate personal information, though the term was left undefined in CCPA and CPRA. The App Association hopes forthcoming regulations will clarify this key term and will harmonize approved business response procedures with existing procedures relating to the right to delete.

Information to Be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)

CPRA expands the 12-month disclosure period for a consumer’s right to know. Consumers may request to know about any new personal information collected or processed on or after January 1, 2022, even if that information is more than 12-months old at the time of the request, subject to certain exceptions to be detailed in regulation. The App Association urges the CPPA to adopt a common-sense exception inclusive of instances where the business migrated its data prior to the 12-month lookback to new storage facilities or service providers, otherwise does not maintain access to the requested data, or the requested data is no longer accessible without creating a significant cybersecurity risk.

⁹ See California Civil Code §1798.185(a)(16)

Additional Comments

As states around the country continue to introduce and pass comprehensive privacy legislation, the risk for conflicting regulatory frameworks increases. With its forthcoming rulemaking process, the CPPA possesses the opportunity to introduce more standardization into our growing national privacy patchwork and reduce the complexity of existing regulations issued by the Office of the California Attorney General, which already run more than 11,000 words with 59 pages of explanatory notes.

We urge the CPPA to consider how it can adopt a proactive and collaborative approach to its rulemaking and enforcement activities in the future. Colorado's privacy law, for example, authorizes its chief enforcer, the state Attorney General, to create rules that allow it to periodically issue opinion letters and/or interpretive guidance that carry a good faith reliance defense for businesses. This framework can be particularly advantageous when seeking to clarify the law relative to emerging business practices or use-cases, a key feature given the nature of the dynamic digital marketplace.¹⁰ Other potential areas of harmonization with existing state law not already mentioned include the definition of dark patterns and the process for validating and honoring global opt-out preference signals sent by a platform, technology or mechanism.

IV. Conclusion

The App Association is a strong supporter of privacy regulation that upholds the mission of consumer protection and sets a clear baseline set of expectations for the businesses that are required to comply. From the small business perspective, it is also vital that privacy regulation create a predictable and consistent legal landscape and is scalable such that smaller entities can continue to comply and compete with larger entities. We are hopeful that the CPPA can strike the appropriate balance.

We thank the CPPA in advance for its consideration of our views, and we look forward to engaging further in the future.

Sincerely,

A solid black rectangular box used to redact the signature of Brian Scarpelli.

Brian Scarpelli

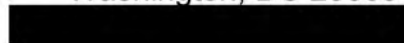
¹⁰ See Colorado Revised Statutes § 6-1-1313(3)



Senior Global Policy Counsel

Matt Schwartz
Innovators Network Foundation Privacy Fellowship Coordinator

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005



From: Divya Sridhar [REDACTED]
Sent: 11/8/2021 11:02:12 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Paul Lekas [REDACTED]
Subject: PRO 01-21 [CPRA Comments due 11-08-21]
Attachments: CPRA_CommentLetter_Final_110821.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Dear Ms. Castanon and others at the California Privacy Protection Agency,

Thank you very much for the opportunity to submit our comments on CPRA proposed rulemaking. Please see attached.

We would be happy to share additional feedback, as appropriate.

Best,
Divya Sridhar



Divya Sridhar, Ph.D.
Senior Director, Data Privacy

[REDACTED]
Siia.net



November 8, 2021

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

RE: Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020

Dear Ms. Castanon:

The Software & Information Industry Association (SIIA) appreciates the opportunity to submit comments about Proposition 24, The California Privacy Rights Act of 2020 (CPRA), which extends the California Consumer Privacy Act of 2018 (CCPA).

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include nearly 450 companies, many based in California or primarily serving California residents. Our members include a range of broad and diverse digital content providers and users in specialized content industries, academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. On behalf of our members' wide interests and services, SIIA has long advocated for privacy protections.

Our members publish a variety of information projects including scientific, technical and medical journals, business to business publications, and databases of news articles and court decisions. They depend on the First Amendment-protected vibrant public domain consisting of both information released by the government and that which is widely available in private hands. The transmission of publicly available information is fully protected by the First Amendment, and we are gratified that CPRA fixed the CCPA's free speech defects. The CPRA revises the definition of personal information (and, separately, the definition of sensitive personal information), to exempt publicly available information from its definition.¹

Our comments focus on honing the practical aspects of implementing CPRA, particularly as it concerns the wide range of members we serve. We also identify compliance-related challenges raised by several of the rulemaking topics. Our comments reinforce two specific recommendations on behalf of our members regarding amendments to CPRA: 1) revise and

¹ CA Civ Code §1798.140 (v) (2) - Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

more narrowly define the term “sensitive personal information”, to avoid first amendment conflicts; and 2) determine the focus, scope and impact of automated decision-making in order to determine how its output is governed and implemented under CPRA.

1. Clarify CPRA’s Requirements with Respect to Limiting Use and Disclosure of Sensitive Personal Information

First, our members agree with the proposition that consumers should be able to opt-out of the sharing and sale of personal information when it violates reasonable expectations of privacy. But, as it concerns notifying consumers about businesses’ use of their information, our members recommend a streamlined approach. CPRA requires companies to provide a clear link allowing consumers to limit the business’ use of their sensitive personal information.² We recommend a simpler process of operationalizing this, by grouping this option with other consumer rights, rather than having to comply with this aspect of the rule as a standalone requirement.

Second, CPRA defines “sensitive personal information”³ to include a wide range of personal information, which is inclusive of: highly identifiable information that imposes a high risk; personal information that may already be governed by existing privacy laws; and lower-risk information that appears to be closely tied with publicly available information. As a practical matter, businesses may not be able to fulfill a consumer’s request to access, limit and delete sensitive personal information (and certain personal information) if the use is reasonably necessary to fulfill a business or service-related obligation, or in circumstances where security and integrity may be compromised. CPRA explicitly adopts exemptions for businesses to comply with consumer’s rights, if the action would disrupt the business’ ability to exercise or defend legal claims.⁴ CPRA also includes business exemptions for deleting consumers’ personal information, in the instances where security and integrity are at odds.⁵ Therefore, it would be beneficial for the Agency to extend a similar protection with respect to the consumers’ right to access their personal information, when security or integrity of the business are at question. The Agency could do so by clarifying that security or integrity are an example of such an exemption to defend a legal claim. Circumstances where businesses can be exempt from fulfilling such requests could include: conducting biometric screenings for authentication purposes, providing fraud prevention or anti-money laundering services, providing age-appropriate content to minors, and participating in similar security and compliance-related activities. These activities may involve third parties and service providers

² CA Civ Code § 1798.135 (2018). Amended by Proposition 24.

³ CA Civ Code § 1798.140 (ae) (1-3): “Sensitive personal information means personal information that reveals: (A) A consumer’s social security, driver’s license, state identification card, or passport number; (B) A consumer’s account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) A consumer’s precise geolocation; (D) A consumer’s racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) The contents of a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication; (F) A consumer’s genetic data.”

⁴ CA Civ Code § 1798.145. Exemptions.

⁵ CA Civ Code § 1798.105. Consumers’ right to delete personal information.

working to fulfill these obligations and allowing customers the opportunity to opt-out would not be plausible.

A separate but related area for potential revision is to exempt inference-based data out of the definition of personal information. As currently written, personal information includes inferences drawn “from any of the information used to build a profile about a consumer, which include the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes⁶”. From a practical standpoint, businesses can use a combination of some sensitive personal information (e.g., trade union membership) and publicly available data (e.g., public records) to build inferences, probabilities, correlations, or couple publicly available data with proxy data (e.g., zip codes) to compile such inferences. If inferences are built from publicly available data and a combination of other personal and sensitive personal information, they should be exempt. Otherwise, there is a risk of regulating “potentially” sensitive personal information, which has not been fully validated as such.

The UK Information Commissioner’s Office (ICO) provides further clarification about the situations when inference-based data should not be considered a “special category” of information⁷, a term which may be comparable to CPRA’s enforcement of sensitive personal information. The ICO suggests that the determination of whether processing inference-based data would trigger GDPR Article 9⁸ is dependent on two factors: the level of certainty of the inference and the intent behind the inference. For example, inferences that are educated guesses would not trigger Article 9, whereas inferences processed specifically to treat someone differently on the basis of that inference would do so. It is important for CPRA to capture these nuances when it comes to implementation. Using the ICO’s guidance is a relevant and logical model for the Agency to provide guidance, after stakeholder input, regarding appropriate use of inference-based data.

Inference-based data is the backbone of many businesses providing tailored or niche services, including profiling (discussed in detail, next) that require a range of information to fulfill a business obligation. Further, by allowing consumers to opt-out of the sharing and sale of inference-based data, it would significantly limit consumer choice and perpetuate inequities if only some consumers limit the sale of their data -- data that is pivotal to businesses that use this data to provide tailored services.

A more focused definition of sensitive personal information can be found in Virginia’s privacy law, the Virginia Consumer Data Protection Act (VCDPA)⁹, which includes the most

⁶ CA Civ Code § 1798.140 (v)(1)(K).

⁷ [What is special category data?](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7) UK Information Commissioner’s Office. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7>

⁸ [Art. 9 GDPR – Processing of special categories of personal data - General Data Protection Regulation \(GDPR\)](https://gdpr-info.eu/art-9-gdpr/) (gdpr-info.eu). <https://gdpr-info.eu/art-9-gdpr/>.

⁹ [VCDPA](#) defines sensitive information to include: “Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health; diagnosis, sexual orientation, or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; the personal data collected from a known child; or precise geolocation data.”

relevant and high-risk personal information to avoid overbreadth and overreach. The VCDPA takes a different approach than CPRA: it excludes lower risk information, such as trade union membership, and does not include inference-based data in the definition of personal information.

We also note that proposing a narrower definition of sensitive personal information in CPRA that excludes driver's license, passport, and financial information would avoid inherent under sampling challenges that stem from collecting data on historically disadvantaged communities, because this type of information may not exist, may be less likely to exist, or may be less likely to be accurate when collected on these populations¹⁰. Some of this data is already governed by other laws (HITECH Act, HIPAA, GLBA, and others) and therefore can be exempted. We should avoid making policy decisions based on data that is not representative or could be processed and used in unbalanced and inappropriate ways.

2. Establish a Principles-Based Approach to Automated Decision-Making Technology, Focused on Fully-Automated Decision-Making Affecting Legal Rights with a Tailored Consumer Opt-Out

We urge the Agency to exercise prudence in approaching regulations on “automated decision-making technology,” a concept that has no predicate in California statute or regulation. Automated technologies are used to render billions of decisions each day. Yet most of these decisions are not sufficiently tied to legal rights of natural persons and, we submit, have no meaningful effect on consumers to out-balance the potentially significant consequences that expansive rulemaking in this area will have on California and its residents.

Regulation of automated decision-making should, to the maximum extent possible, be both risk-based and technology-neutral. Because not all automated decision-making creates the same privacy risk, regulations should be tailored to the harms created by that risk. A standard that presumes that the use of automated decision technology is undesirable would hamstring many beneficial uses of automated technologies. Instead, we respectfully suggest that regulation in this context focus on decisions made solely on an automated basis that produce legal or similarly significant effects on a consumer. This will help ensure that California's rules provide an ongoing privacy framework to withstand technological advances.

In applying this approach, we respectfully offer the following guiding principles.

A. Distinguish Between Automated Decision-making and Automated Decision-making Technology

First, the Agency should pay close attention to the distinction between *automated decision-making*, and *automated decision-making technology* (and respective engines) *that drive the decision-making process*. The Agency's phrasing of the questions within Topic 2 suggests awareness of this distinction. Respectfully, we submit that the Agency should focus its rulemaking on the *decisions* that are generated by automated processes rather than on the

¹⁰ Big Data and discrimination: perils, promises and solutions. A systematic review. Journal of Big Data. SpringerOpen. <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0177-4>

technology itself. Regulating technology more broadly will have significant, unforeseen (and negative) consequences for consumers and businesses alike.

Companies across a wide range of industries today use technology to generate or inform a broad set of decisions. Automation serves a range of purposes, from personalizing and customizing content for groups of people and specific purposes, authenticating mobile apps, and providing fraud-detection alerts and security alerts and features, which powers basic processes in banking, retail, security, tech, publishing, automobile, and other industries.

B. Decisions Should be Based on Impact on Natural Person's Rights

Second, the Agency's approach to automated decision-making should be guided by clear objectives. The CPRA already provides the outer limits of those objectives. Specifically, the statute ties rulemaking on automated decision-making technology to the definition of "profiling":

"Profiling" means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."¹¹

This definition indicates a concern with how automated processes may be used to profile natural persons in a manner that has a direct effect on that natural person. Yet the definition of "profiling" leaves open what sort of "decisions" should be subject to regulations.

We recommend that the "decisions" should be those that have a direct effect on the legal rights of the natural person subject to automated decision-making. This approach is informed by the approach taken by the European Union. Article 22 of the GDPR protects consumers from decisions "based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."¹² We recommend that any rulemaking on automated decision-making be closely tied to those situations in which ***profiling is done through automated processes that have a direct effect on the legal rights of a natural person.***

C. Tailor Determination of Impact to Risk-based Approach

Third, we recommend the Agency focus its rulemaking on fully automated decisions – those that do not involve any human support. Similar to the intent of GDPR Article 22, the Agency could clarify that consumers have an opportunity to opt-out of automated

¹¹ CA Civil Code § 1798.140(z).

¹² [Art. 22 GDPR](https://gdpr-info.eu/art-22-gdpr/) – Automated individual decision-making, including profiling - General Data Protection Regulation (GDPR) (gdpr-info.eu). <https://gdpr-info.eu/art-22-gdpr/>

decision-making, only in instances when the consumer faces a “legal or similar effect” that is based on the automated decision-making (and does not involve human input or intervention). This creates a narrowly tailored, situation-based approach to opt-out that would require a high level of necessity, so as not to bog down businesses with unnecessary consumer requests to opt-out of routine, automated transactions.

Taking this approach one step further, and to avoid the situational vagueness that is embedded in the GDPR, we recommend that additional input be gathered to aggregate a list of specific use cases for when opt-out would be necessary and considered to have a legal or similar effect. The agency could share this list with businesses and consumers to provide further clarity and examples of when the opt-out would apply. GDPR Article 22 also allows some exemptions with regard to this right, including using data to enter into contracts and processing that is authorized by law or in circumstances when explicit consent is granted by the consumer.¹³

We propose narrowing opt-out requests to scenarios based on the potential for significant impact to the consumer, and using certain criteria to determine the impact, such as: a) whether the decision-making is based on fully or partially automated technology; b) the level of risk and material harm the decision would impose on the consumer; c) whether human input is a part of the decision-making process; d) the benefits to the business and the public from the use of the technology; and e) the irreversibility of the decision. A risk-based approach could allow consumers to opt out of profiling in life-altering or particularly challenging situations, such as access to essential goods or services (for insurance, healthcare, criminal enforcement, or other related purposes and activities).

Using such an approach, consumers should also be granted the right to obtain human intervention and the right to challenge decisions with legal or similarly significant effects, aligned to GDPR Article 22(3). Therefore, we recommend inclusion of an appeal process to ensure appropriate recourse. The appeal process would allow for additional consumer support in understanding the information granted to them and addressing any changes they require with regard to opting out of the information or opting back into the automated process, as needed. Additional, business process-related concerns about authenticating and answering consumer requests – including the types of information to be provided by the business, how to make this information most useful and readable to the consumer in Plain English, and how to standardize this information – could be answered through an additional request for stakeholder input or a rulemaking process.

D. Overly Prescriptive Rules on Profiling May Limit Innovation

Fourth, while we appreciate the steps that the legislature took to carve out publicly available information, we remain concerned about the manner in which the statute’s broad limitations on “profiling” may inadvertently chill the expression of protected expression. The statute defines profiling as “any form of automated processing of personal information... to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation,

¹³ Artificial Intelligence (AI) and the GDPR - Part one - Data Protection - [PWC UK blogs](https://pwc.blogs.com/data_protection/2019/01/artificial-intelligence-ai-and-the-gdpr-part-one.html).
https://pwc.blogs.com/data_protection/2019/01/artificial-intelligence-ai-and-the-gdpr-part-one.html



health, personal preferences, interests, reliability, behavior, location or movements.¹⁴ It is not difficult to envision, for example, an investigative reporter who might consult one of our members' products to identify a potential source through a combination of covered and publicly available information. All kinds of research draw inferences from both types of information, and we do not believe the intent of the legislature was to chill it unintentionally. Once again, we believe that the Agency's efforts would benefit from a more detailed and specific administrative record, by attempting to define these circumstances in more detail.

Notwithstanding these principles, we believe there are unique considerations when analyzing data generated by automated decision-making technologies and recommend the Agency host additional stakeholder input and hearings specifically to discuss this issue. To both adequately protect privacy and allow for innovation in the use and development of artificial intelligence, we urge policy makers to engage in fact-finding to fully understand this developing but technologically essential ecosystem.

In sum, we believe that changes along the lines above will both make CPRA a national model and support increased interoperability with other state consumer privacy laws. We thank you for the opportunity to submit comments. Please do not hesitate to reach out with further questions on this or other consumer privacy-related matters.

Respectfully submitted,

Paul Lekas, Senior Vice President for Global Public Policy

Divya Sridhar, Senior Director for Data Policy

Software & Information Industry Association

¹⁴ CA Civil Code, sec. 1798.140 (z)

From: Elizabeth Galicia [REDACTED]
Sent: 11/8/2021 11:33:40 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Nicola White [REDACTED]
Subject: PRO 01-21 from Beeban Kidron/5Rights
Attachments: Public comment for the California Privacy Protection Agency.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Thank you!

Public comment for the California Privacy Protection Agency

Baroness Beeban Kidron, Chair 5Rights Foundation

Bravo to California. It's a landmark moment for data privacy that the California Privacy Protection Agency exists and has a groundbreaking role in implementing and enforcing the state's privacy law. Seeing this important work commencing I wanted to add my experience, albeit from the UK, that I introduced into United Kingdom law, the Age Appropriate Design Code.

Children are being monetized by the digital products and services focused on the relentless pursuit of every ounce of their attention and data, and whilst that seems somewhat abstract, it has a palpable effect on children's digital experience since many of the features of data optimisation put children at risk. In my submission below I set out the journey we have gone on in the UK, and hope that it is of use to you in your deliberations.

The Age Appropriate Design Code (Code) was intended to be, and is in practice, a mechanism for ensuring safety by design in platforms. And while CCPA and CPRA after it are also aiming to minimize harm, particularly to vulnerable populations of which children certainly are, the Code sets itself a child-centred view of digital products and services and reimagines them in the 'best interests' of the child.

I am Baroness Beeban Kidron, a crossbench (independent) member of the House of Lords. In that capacity I have sat on the House of Lords Communications and Digital Committee, the Digital Democracy committee inquiry, and am currently a member of the pre-legislative scrutiny committee of the UK's flagship Online Safety Bill. I am also co-founder and deputy chair of the All-Party Parliamentary Group for Digital Regulation and Responsibility which numbers almost 100 parliamentarians, across both houses and from all parties. Outside parliament, I am Chair of 5Rights Foundation, a nonprofit that does groundbreaking work around the world to make systemic changes to digital systems in order to protect children. 5Rights developed a Child Online Protection Policy for the Government of Rwanda, has supported multiple nation state efforts to develop data protection regimes, and is working in partnership with the Institute for Electrical and Electronics Engineers (IEEE) to co-create Universal Standards for Children and for Digital Services and Products. Most recently, 5Rights supported the Committee on the Rights of the Child (UNCRC) in drafting general comment No. 25 (2021) on children's rights in relation to the digital environment. This authoritative document, adopted in March this year, is anticipated to have global significance on the expectations and duties of states and business to children. I also work with international bodies such as the Organization for Economic Cooperation and Development (OECD), UNESCO Broadband Commission and EU organisations on issues such as Artificial Intelligence (AI), child-centred design and data protection.

In 2012, when smartphones began to be priced at a point that allowed a parent to provide this powerful device to a child, childhood fundamentally changed. This device, increasingly glued to their pocket, bedroom, hand and gaze, gave children unfettered access to a world of breathtaking richness and variety. It also gave adults and commercial entities unfettered and unchecked access to children – access that has been ruthlessly exploited.

In the UK, it has been 150 years since we took children out of the chimneys and put them in the classroom – arguably the beginning of what we now conceive of as childhood. Childhood is a journey from dependence to autonomy with its own set of vulnerabilities and learning. Childhood is not a risk-free business, but there is broad consensus that we have a duty of care, which requires us to protect children from foreseeable risks and preventable harms – a duty on us as parents, politicians and businesses. This consensus is taken for granted in the decisions we make about all aspects of children's lives – except the digital world. This is not acceptable. My personal battle and political commitment is to ensure this wrong is put right.

In 2018, as part of the Data Protection Bill, I introduced an amendment to create the Age Appropriate Design Code (AADC). The AADC has some key features. The Code defines a child as any person under the age of 18. This is in stark contrast with the tech sector that has exploited a gap in legislation to treat all 13-year-olds as adults, when any parent or child will tell you that at 13 you are still a child. Similarly, the Code is applicable to services 'likely to be accessed by children' rather than restricting protections to services directed at children. Most children spend most of their time online on services which are primarily designed for adults. Importantly, the Code transfers the responsibility for safety from the child to the product, requiring services to consider, in advance, how their data practices might impact on the user if that user were a child under 18.

The Code is made up of 15 standards, and they carry equal weight. Each has a very specific function, but the central purpose of the Code as a whole is to create an environment in which the choices companies make in their data processing activities are in the best interests of the child, the first provision.

1. Best interests of the child: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.
2. Data protection impact assessments: Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this code.
3. Age appropriate application: Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead.
4. Transparency: The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent, and in clear

language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.

5. Detrimental use of data: Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions, or Government advice.
6. Policies and community standards: Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).
7. Default settings: Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).
8. Data minimisation: Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.
9. Data sharing: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.
10. Geolocation: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others should default back to 'off' at the end of each session.
11. Parental controls: If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.
12. Profiling: Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).
13. Nudge techniques: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections.
14. Connected toys and devices: If you provide a connected toy or device, ensure you include effective tools to enable conformance to this code.
15. Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

The 15 provisions of the Children's Code are interconnected and interdependent – but together they offer children a high bar of data protection, including protections from revealing their location, using a child's personal data to deliver detrimental material, or deliberately nudging them to give up their privacy.

During the summer as the deadline to compliance with the Code approached, there were a number of eye-catching announcements, including:

- Instagram will no longer allow unknown adults to direct message those under 18¹ and TikTok has switched off direct messaging altogether for under 16s²
- Children under the age of 16 will have their accounts set to private by default on TikTok
- Google³ and Facebook⁴ will stop behavioural advertising to children
- Google's SafeSearch will be turned on by default for all under 18s, and will be extended to cover children's interactions with Google Assistant on shared devices⁵
- YouTube will turn off auto-play, preventing children seeing an endless stream of videos⁶
- All apps in the 'Kids' category of the Apple App Store must protect children's data and provide only age-appropriate content, and must not send personally identifiable information or device information to third parties⁷
- Google Play Store now prevents accounts registered to under 18s from viewing and downloading apps rated as adult-only
- And a whole host of wellbeing measures such as turning off notifications and on time outs

These changes are not only being made in services' UK operations but are being implemented globally. They enhance children's online experiences by default, rather than relying on parental controls or on locking children out of digital spaces. The Code has demonstrated how the digital world can be improved and redesigned so that it is optimised for the protection of children rather than for ever more 'engagement.' California has the opportunity to reinforce these gains and assure that children in the United States start to have equal protections online with their peers in the UK.

What is central to understanding the impact of the Code is that while each individual change is in itself an increment to a better and safer digital experience for children – it is

¹ <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community>

² <https://newsroom.tiktok.com/en-us/strengthening-privacy-and-safety-for-youth>

³ <https://blog.google/technology/families/giving-kids-and-teens-safer-experience-online/>

⁴ <https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/>

⁵ <https://blog.google/technology/families/giving-kids-and-teens-safer-experience-online/>

⁶ <https://blog.youtube/news-and-events/new-safety-and-digital-wellbeing-options-younger-people-youtube-and-youtube-kids/>

⁷ <https://developer.apple.com/app-store/kids-apps/>

the 'by design' nature of the Code that has shown the world that digital products and services are human made and can be made safe if they are optimised to do so.

The full impact of the Children's Code remains to be seen, but in a recent conversation with one of the major platforms, I was told that all their product teams now have to consider the Code's 15 provisions, including its overarching requirement to process children's data in "the best interests of children," and if I might quote the Code directly, which states that: "It is unlikely that the commercial interests of an organization will outweigh a child's right to privacy."⁸

These baseline protections are overwhelmingly popular with the public that is tired of industry norms that promote intrusive and addictive design practices, or exacerbate and recommend harmful material, and they are sickened by the idea that a child's real time location can be tracked by a stranger – or predator.

As I have worked on this issue around the world, gradually policymakers have come on board – but still parents, teachers and very often children themselves feel helpless to understand how they are being manipulated. We do not accept this manipulation of children anywhere else - we must not accept it online. The reason that parents, teachers and children feel overwhelmed is that this is not a problem that parents, teachers or kids can solve on their own. A system designed to extract every ounce of a child's attention, expose them to an infinite public and encourage them to get lost in the mirror of anxiety, is not healthy. The tech sector has the ability to raise the ceiling and to give children back their childhood – but it is up to legislators to insist on the floor of behaviour below which they must not go.

There is a big and growing gap between the needs of children and the regulation in place. The digital world has transformed, but our protections for children have not kept pace. The US is home to many of the companies that dominate the sector, and what lawmakers in the US do for children will ricochet around the world. California is best placed to act on a comprehensive set of actions to protect children with its privacy laws and an agency charged with implementation and rulemaking.

I am at your disposal ready to support your efforts. The AADC was borne out of four years of research and stakeholder input and has as its foundation a child development framework that supports the well-being of children at every age. While the UK has taken steps, many of the companies that set the culture and the practice of the digital world reside in California, we can drive good behaviour and enforce against bad behaviour in the UK, but unless and until the US joins us in making data protection (safety by design) an enforceable norm, then children's privacy safety and wellbeing - is at the whim of commercial companies that have repeatedly been found to treat all three with profound disregard. At 5Rights we are dedicated to building the digital world young people deserve, and we stand ready to support California to do the same.

⁸ <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/>

From: Diederich, Damon [REDACTED]
Sent: 11/8/2021 11:30:19 AM
To: Castanon, Debra@CPPA [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b9766af8eba04290bfa5ae3e150c60e7-Castanon, D]; Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 Comments in Response to Invitation for Preliminary Comments
Attachments: 2021-11-08_LTR_DIEDERICH_(CDI)_TO_CASTANON_(CPPA)_RE_PRELIM_REG_COMMENTS....pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Good morning-

Attached are comments in response to the September 22nd Invitation for Preliminary Comments regarding Proposition. 24.

Please contact me with any questions. Thank you!

-DD

Damon Diederich
Attorney III / Privacy Officer
California Department of Insurance
300 Capitol Mall, FL11
Sacramento, CA 95816
[REDACTED]

CONFIDENTIALITY NOTICE: This communication may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use, or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.



RICARDO LARA
CALIFORNIA INSURANCE COMMISSIONER

November 8, 2021

VIA ELECTRONIC MAIL

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

regulations@coppa.ca.gov

SUBJECT: Response to Invitation for Preliminary Comments re California Privacy Rights Act of 2020

Dear Ms. Castanon:

The California Department of Insurance ("CDI" or "Department") submits the following comments, in response to the California Privacy Protection Agency's ("Agency") September 22, 2021 Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 ("Prop. 24").

Part of the Agency's rulemaking authority is to review the California Insurance Code and related regulations pertaining to privacy, and via regulation, apply to insurance companies only the portions of Prop. 24 which provide greater privacy protection than the Insurance Code and regulations.¹ Prop. 24 also reaffirms the jurisdiction of the Insurance Commissioner over insurance rates and pricing.²

The Department is responsible for regulating the business of insurance within the State of California, including the activities of insurance companies, agents and brokers, and companies providing services to those entities, among others. As part of that mandate, CDI administers the Insurance Information and Privacy Protection Act ("IIPPA"),³ and the related Privacy of Nonpublic Personal Information regulations ("PNPI").⁴

¹ Civil Code ("CIV") §1798.185(a)(21). The Department notes that, while the rulemaking mandate contained at CIV §1798.185 is directed to the Attorney General, the Agency accedes to that authority, per CIV §1798.199.40(b).

² Id.

³ Insurance Code ("INS") §791, et seq.

⁴ 10 CCR 2689.1, et seq.

Revision of Insurance Privacy Statutes

The IPPA is in the initial stages of being revised, and these revisions are likely to lead to changes in the PNPI regulations. By way of background, the Department participates in the National Association of Insurance Commissioners (“NAIC”), which serves as a regulatory college and policy coordination body for the insurance commissioners of the states and territories of the United States.⁵ Among the NAIC functions is the development of Model Acts which membership may adopt. California’s IPPA is based on the NAIC Insurance Information and Privacy Protection Model Act; NAIC Model Act #670.

The NAIC is in the process of soliciting regulator and stakeholder comments on revisions to Model #670. For the last two years, CDI has participated in a working group of insurance regulators charged with determining the applicable scope of privacy protections for insurance consumers. The working group report is scheduled to be presented this December and will likely recommend amendments to Model #670.

Because California’s IPPA is based on Model #670, the IPPA will likely be amended in the next 2-4 years, after the adoption of revisions to the NAIC Model, or development of a new model. The PNPI regulations are based on the IPPA, and are also likely to be revised.

Due to the impending amendment of applicable insurance privacy statutes, the Department respectfully requests that the Agency provide the Department with the opportunity to work with the Agency before the adoption of any regulation that would implement the insurance privacy subdivision of the Civil Code. Because the NAIC is actively working to amend Model #670, which will affect the IPPA and related PNPI regulations overseen by CDI, close coordination between the Department and the Agency is critical. This will avoid duplicative efforts on the part of the Agency and the Department, and promote certainty on the part of consumers and regulated entities.

Cybersecurity Audits, Risk Assessments, and Agency Audit Authority

As part of the September 22 Invitation for Preliminary Comment, the Agency requested discussion on auditing and risk assessment by entities subject to Prop. 24, as well as audits to be conducted by the Agency.

Internal Cybersecurity Audits and Risk Assessments

As part of the CDI PNPI regulations, insurance entities are required to design and implement an information security program.⁶ Such program is to be designed around the “CIA Triad” of Confidentiality, Integrity, and Availability,⁷ based on a risk assessment conducted by the entity⁸;

⁵ Due to the 1945 enactment of the McCarran-Ferguson Act (15 U.S.C. §1011 – 1015), regulation of the business of insurance is generally reserved to the states.

⁶ 10 CCR §2689.14.

⁷ 10 CCR §2689.15.

⁸ 10 CCR §2689.16.

once established, entities are required to test and monitor their information security program, consistent with intervals determined by the entity's risk assessment.⁹

As discussed above, the Department expects the PNPI regulations will change, based on revisions to NAIC Model #670 and the IIPPA. These changes to Model #670 will likely lead to a change in law for many – if not all – insurance regulatory authorities within the United States and its territories. Therefore, insofar as Civil Code section 1798.185, subdivision (a)(21) directs the Agency to review existing Insurance Code provisions and regulations relating to consumer privacy and also reaffirms the Insurance Commissioner's jurisdiction over rates and pricing, the Department respectfully requests the opportunity to work with the Agency before the adoption of any regulation that would implement this subdivision of the Civil Code. Because the NAIC is actively working to amend Model #670, which will affect the IIPPA and related PNPI regulations overseen by CDI, close coordination between the Department and the Agency is critical.

Agency Audit Authority

The Agency has the authority to: compel testimony and the production of books and records, including during the exercise of the Agency's audit authority¹⁰; to develop regulations relating to the exercise of the Agency's audit authority¹¹; and to appoint a Chief Auditor.¹²

The Department has broad authority to conduct examinations of all business and affairs of regulated insurance entities,¹³ including special authority to examine the privacy practices of a regulated entity,¹⁴ and audit an entity's compliance with cybersecurity program requirements of the PNPI regulations.¹⁵ CDI examination authority includes the ability to: conduct a full examination of the affairs of a regulated entity, including compliance with all applicable laws;¹⁶ compel sworn testimony and production of books and records;¹⁷ and engage qualified outside experts when necessary.¹⁸ The Department audits regulated entities' privacy and security compliance as part of the scheduled examinations done by the Department's Market Conduct Division.

The Department respectfully requests that, to the greatest extent possible, the Department and the Agency endeavor to schedule audits of insurance entities to minimize duplicative efforts or disruption to the entities being audited.

⁹ 10 CCR §2689.17.

¹⁰ CIV §1798.199.65.

¹¹ CIV §1798.185(a)(18).

¹² CIV §1798.199.40(f).

¹³ INS §729, et seq.

¹⁴ INS §791.14.

¹⁵ 10 CCR §2689.20.

¹⁶ INS §733.

¹⁷ INS §734.

¹⁸ INS §733.

Health Information Collection: Reducing Disparities in Health Coverage

The Department is currently a member of the NAIC Special Committee on Race and Insurance.¹⁹ The committee's work includes an initiative to reduce disparities in access to health coverage; Workstream Five of the committee is focused on promoting equity through improving access, including remedying disparate impacts on historically marginalized groups. In order to accomplish these aims, Workstream Five is developing a white paper regarding best practices for collection and nondiscriminatory use of race and identity data of insureds and providers.

We believe that any regulatory action by the Agency should consider these health data collection activities. The Department encourages the creation of a more formalized communication process between our organizations so that the Department can coordinate and share information with the Agency concerning these national efforts to promote equity and improve access.

Conclusion

As discussed above, the Department respectfully requests that Agency rulemaking with respect to insurance privacy be conducted in coordination with the Department, particularly in light of the NAIC's current evaluation of changes to model insurance privacy statutes and regulations. The Department supports the Agency's activities to protect consumer data privacy and welcomes frequent engagement in furtherance of our respective privacy mandates.

Sincerely,

A solid black rectangular box used to redact the signature of the Privacy Officer.

Damon Diederich
Privacy Officer / Attorney III

¹⁹ https://content.naic.org/cmte_ex_race_and_insurance.htm

From: Sebastian Zimmeck [REDACTED]
Sent: 11/8/2021 12:21:56 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: Comments_on_the_Proposed_Rulemaking_Under_the_California_Consumer_Privacy_Act_of_2020_(Proceeding No. 01-21).pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Dear Debra,

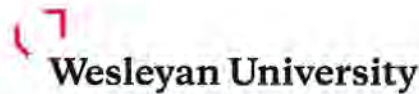
Please find attached my comments on the proposed rulemaking under the California Consumer Privacy Act of 2020 (Proceeding No. 01-21).

Thank you for your consideration.

Best regards,

Sebastian

We launched [Global Privacy Control](#)
[privacy-tech-lab](#), Wesleyan University



Mathematics and Computer Science Department

265 Church Street
Middletown, Connecticut 06459
860 685 2620 Fax: 860 685 2571
www.math.wesleyan.edu

Sebastian Zimmeck
Assistant Professor of Computer Science

November 8, 2021

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

Dear Debra,

As one of the initiators of the Global Privacy Control (GPC) protocol [1], I would like to comment on the proposed rulemaking under the California Consumer Privacy Act of 2020 (Proceeding No. 01-21), 5d How businesses should process consumer rights that are expressed through opt-out preference signals [2], as follows.

1. Section 1798.135(e) of the California Consumer Privacy Act

Section 1798.135(e) of the California Consumer Privacy Act (CCPA) allows consumers to authorize another person to opt-out of the sale of personal information on their behalf via opt-out preference signals. The details of such opt-outs are to be specified in regulations that will be adopted by the California Attorney General. Section 1798.135(e) reads as follows:

A consumer may authorize another person to opt-out of the sale or sharing of the consumer's personal information and to limit the use of the consumer's sensitive personal information on the consumer's behalf, including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b), indicating the consumer's intent to opt out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General regardless of whether the business has elected to comply with subdivision (a) or (b). For purposes of clarity, a business that elects to comply with subdivision (a) may respond to the consumer's opt-out consistent with Section 1798.125. [emphasis added]

Section 1798.135(e) is a crucially important provision for consumers to exercise their opt-out rights via privacy preference signals by a representative, especially, as it applies regardless of whether a business has elected to comply with 1798.135 (a) or 1798.135 (b). However, without further clarification in the regulations, I am doubtful that it will be of much use for consumers, at least, if the requirements for the representatives acting on behalf of the consumers are interpreted too narrowly.

2. Clarify in the Regulations That the Consumer's Representative Can Act Through Automated Software, especially, Software on the Consumer's Computer

Websites usually rely on identifiers, such as cookie identifiers or login credentials, to keep track of a consumer's opt-out status. The representative would need to have access to these identifiers to facilitate the opt out for a consumer. Requiring a consumer to send such identifiers to a representative is a potential security risk and highly impractical. For example, consumers would need to look up individual cookie identifiers on their browser, which may not be easily accessible, and provide those to the representative. It would be much simpler if consumers could download software for installation on their computers by which representatives could access the required information on-device and process it from there. For example, representatives could provide dedicated opt-out browser extensions. In fact, if their browsers contain opt-out functionality, browser vendors could also act as representatives. This way the privacy preference signaling could be automated. Using cloud-based opt-out functionality may be an option as well to help consumers exercising their opt-out rights.

3. Clarify in the Regulations That the Consumer Can Authorize the Representative via the Representative's Terms of Service or Other Electronic Contract Without Any Additional Requirements

Representatives can exercise consumers' opt-out rights via opt-out preference signals if they are authorized to do so. If consumers want a representative to opt-out on their behalf, section 1798.135(e) requires them to "authorize another person." Thus, the regulations should clarify what qualifies as an authorization in the context of section 1798.135(e). In particular, consumers should be able to authorize representatives via the representatives' terms of service or other electronic contracts that the consumers agree to. Otherwise, it would be necessary to authorize representatives by a dedicated authorization process, which the average consumer would likely not engage in. In case of a browser vendor acting as a representative the website receiving the opt-out request would also be aware of the consumer's authorization via the user agent indicating the browser the consumer uses. It would be clear to websites that all consumers using a browser with opt-out functionality turned on and language in its terms of service that the vendor acts as representative are authorizing the browser vendor for purposes of section 1798.135(e). For browser extensions and other non-browser software a link to the website with the terms of service could be sent to the website together with the privacy preference signal.

Thank you for the opportunity to comment. I am available for further questions and clarifications.

Sincerely,



Sebastian Zimmeck

[1] [Global Privacy Control \(GPC\)](#).

[2] [Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 \(Proceeding No. 01-21\)](#).

From: Chris Pedigo [REDACTED]
Sent: 11/8/2021 12:43:44 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: DCN Comments re CPRA (Pro 01-21)
Attachments: DCN Comments to CPPA re CPRA Rulemaking 2021-11-08 - Final[1].pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Please find the attached comments from Digital Content Next in response to your solicitation for comments on the California Privacy Rights Act (CPRA). Please let me know if you have any trouble with this document or if there are any follow up questions.

Sincerely,

--

Chris Pedigo
SVP, Government Affairs
Digital Content Next
[REDACTED]

Follow us on Twitter: [@DCNorg](#)
[Sign up](#) for our weekly newsletter, InContext, for insights in digital media.



November 8, 2021

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

RE: PRO 01-21

To Whom It May Concern,

We appreciate the opportunity to comment as you develop regulations to implement the California Privacy Rights Act (CPRA). Digital Content Next (DCN), representing many of the Internet's most trusted and respected publishing brands, appreciates the opportunity to submit comments in the above-captioned proceeding. Founded in 2001, DCN is the only trade organization dedicated to serving the unique and diverse needs of high-quality digital content companies that manage trusted, direct relationships with consumers and marketers.¹ DCN's members are some of the most trusted and well-respected media brands that, together, have an unduplicated audience of 223,098 million unique visitors or 100 percent reach of the U.S. online population.

In response to your solicitation, we offer the following comments on behalf of premium publishers and look forward to working with you to ensure proper enforcement of the CPRA.

Opt-Out Signals Application to Downstream Companies

Section 1798.135 (f) clearly lays out that third-party companies collecting a consumer's personal information from a website must respect a consumer's opt-out request when the website owner passes along the opt-out signal. Indeed, the legislative text lays out that a third-party company shall revert to the role of a service provider. Specifically, the text says, "*If a business communicates a consumer's opt-out request to any person authorized by the business to collect personal information, the person shall thereafter only use such consumer's personal information*

¹ See <https://digitalcontentnext.org/membership/members/> for a listing of our current members.

for a business purpose specified by the business, or as otherwise permitted by this title, and shall be prohibited from: (1) selling or sharing the personal information; or (2) retaining, using, or disclosing such consumer's personal information: (A) for any purpose other than for the specific purpose of performing the services offered to the business, (B) outside of the direct business relationship between the person and the business, or (C) for a commercial purpose other than providing services to the business."

Section 1798.135 (g) expands on the previous provision by noting that a publisher shall not be held liable for any violations by downstream partners unless they have actual knowledge or reason to believe that a violation will occur.

Taken together, these provisions recognize the complex and dynamic nature of the digital ecosystem. In the case of a publisher's website or app, a myriad of third-party companies play important roles in combatting fraud, ensuring a smooth consumer experience, and delivering advertising among many other things. Crafted with this complexity in mind, the CPRA puts the onus and liability to honor a consumer's privacy preferences on the company actually collecting data. As you consider how best to enforce the CPRA's provisions and conduct audits to ensure proper compliance with the CPRA, we urge you to put the onus on each company for its own data collection and use practices and to avoid putting publishers in a position of having to serve as the enforcers of privacy law.

Global Privacy Controls

We are pleased that the CPRA explicitly allows for consumers to use an opt-out preference signal and DCN has been supportive in the development of the Global Privacy Control (GPC), as one potential mechanism, to facilitate users being able to clearly express their privacy preferences. This is especially important as it facilitates being able to communicate to companies with which they are not choosing to interact in a certain context. As with the current GPC, we don't believe this signal should require a user to take specific action to confirm or authenticate the signal. Its purpose is to eliminate consumer friction and most rapidly align with the consumer's expectations without requiring additional data to be supplied or effort to be taken. These opt-out signals may be turned on by default as written in the law especially to the extent that the signal is clearly marketed to the consumer as a privacy-enhancing tool. However, publishers are concerned that browser or device companies may seek to promote their own preference signals to unfairly favor their own business.

However, while we support the intent of the CPRA, there may be a lack of clarity around what companies should do when they receive these signals. Section 1798.135 (a) requires businesses to provide links for consumers to exercise their rights to "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information." Section 1798.135 (b) states that businesses do not have to comply with (a) if they allow consumers to "*opt-out...through an opt-out preference signal sent with the consumer's consent by a platform, technology or mechanism...*" However, Section 1798.135 (e) requires businesses to honor an "*opt-out request received from a person authorized by the consumer to act on the consumer's behalf...regardless of whether the business has elected to comply with subdivision (a) or (b) of*

this Section.” It is not clear whether the CPRA envisions separate signals and how businesses should react. We agree with the intent of the CPRA to empower consumers with easy-to-use tools to exercise their rights under the CPRA and urge you to provide clarity about how businesses must honor these signals.

Anonymous Audiences

In the Agency’s solicitation, there are a number of questions about how best to allow consumers to exercise their rights under the CPRA. As you craft regulations in this regard, we urge you to consider that a significant portion of consumers visiting a publisher’s website or app are anonymous (not logged in). Honoring rights to limit the sale or sharing of data should be straightforward. However, for a publisher to honor access, correction and deletion rights for anonymous audiences, the publisher would need to collect additional information about the consumer to verify their identity. Our concern is that additional data collection from anonymous audiences would run counter to the goals of the CPRA to protect consumer privacy and could unintentionally create additional security risks.

Consumer Expectations

Regarding Question 1 “Processing that Presents a Significant Risk to Consumers’ Privacy or Security” and Question 6 “Consumers’ Rights to Limit the Use and Disclosure of Sensitive Personal Information,” we urge the Agency to differentiate between processing that is expected by consumers versus processing that is not expected. Consumers sometimes intentionally provide personal information on a website or app with the company they intend to interact. This information is often used to provide direct benefits for consumers (e.g. registration information to read a news article, location data to receive local alerts and personalized content). In other cases, demographic data is collected to measure a publisher’s audience and improve efforts to reach underserved sections of the population. In addition, news publishers often collect demographic data about their audiences and sources to ensure there is a broad diversity of voices in media. These kinds of data uses provide immense benefits to society at little risk to consumers. Generally, data used within the context of the consumer’s relationship with the business is often expected by the consumer and, thus, presents less risk to the consumer’s privacy. However, consumers may not be aware and would certainly not expect that third parties may be processing that information as well for use outside of the context where the information was originally collected. Information collected outside of consumer awareness is not likely expected and, thus, could risk the consumer’s privacy. In addition, this kind of data processing could pose a greater security risk as the third-party company is likely less-dependent upon safeguarding the trust of the consumer.

Finally, it would be useful to harmonize with existing laws such as the European Union’s General Data Protection Regulation (GDPR). Under the GDPR, a Data Protection Impact Assessment 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.

Conclusion

We appreciate the opportunity to provide comments for this proceeding. Please do not hesitate to reach out directly to us if you have any questions or if we can be of service.

Sincerely,



Chris Pedigo
SVP, Government Affairs
Digital Content Next

From: Cindy Sakyi [REDACTED]
Sent: 9/26/2021 11:08:49 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: Comments for Consumer's rights: Selling or sharing

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

To whom it may concern:

Question:

- 1. When it comes to "cross- context behavioral advertising" is this specific to sharing information with social media sites or is it broader than that?**
- 2. Does it include sharing across brands in the same company, for example?**

CSEC. 9. Section 1798.120 of the Civil Code Is amended to read: 1798.120, Consumers' Right to Opt-Out of Sale or Sharing of Personal Information 1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells or shares personal Information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing. (b) A business that sells consumers' personal Information to, or shares It with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the "right to opt-out" of the sale or sharing of their personal information.

Selling: "Sell," "selling," "sale," or "sold," means selling, 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 the business to a third party for monetary or other valuable consideration.

Sharing: "Share," "shared," or "sharing" means sharing, 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 the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business In which no money is exchanged.

Cross-context behavioral advertising- (k) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal Information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally Interacts.

Thank you and I look forward to getting more clarification.
Cindy Sakyi

From: Ginny Kozemczak [REDACTED]
Sent: 11/8/2021 7:25:20 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: IDAC CPPA Public Comment 11.8.21 (2).pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Dear California Privacy Protection Agency:

The International Digital Accountability Council (IDAC) is pleased to submit the following public comment, attached to this email.

Please let us know if you have any questions.

Thank you!

Ginny

--
Ginny Kozemczak

IDAC

Chief of Staff & Policy Counsel

International Digital Accountability Council
digitalwatchdog.org



Comments to the California Privacy Protection Agency By the International Digital Accountability Council

November 8, 2021

California Privacy Protection Agency
915 Capitol Mall, Suite 350A
Sacramento, CA 95814
www.cppa.ca.gov

Introduction

Voters approved the California Privacy Rights Act of 2020 (“CPRA”) last year and it will go into effect January 1, 2023. The law amends and extends the California Consumer Privacy Act of 2018 (“CCPA”) and creates a new agency to implement the law. The California Privacy Protection Agency (“CPPA”) is vested with full administrative power, authority, and jurisdiction to implement and enforce the CPRA. The Agency has invited public comments related to any area on which the Agency has authority to adopt rules.

The [International Digital Accountability Council](https://digitalwatchdog.org/investigations/) (“IDAC”) is an independent watchdog created to improve digital accountability through international monitoring, investigation, education and collaboration with applications, platforms, law enforcement, and more.

In September 2021, we investigated more than 150 mobile health apps, including period-trackers and other “femtech” apps, mental health apps, and fitness and weight loss apps.¹ Our research included technical data flow analysis, as well as an examination of privacy policy disclosure. Our findings showed that many of these apps handle *sensitive personal information*² as defined by the

¹ Our full report will be published on November 15, 2021 and will be found on our webpage: <https://digitalwatchdog.org/investigations/>.

² CA. Civ. Code, § 1798.185(a)(15)(B).

CPRA. Concerningly, however, many of these apps remain unregulated and pose privacy and security risks to individuals. The results of our research provide clear evidence-based policy considerations for the CPPA.

As the rise of [digital health services](#) has rapidly increased, the consumer protections that were put in place during a more analog era no longer extend coverage to protecting our most sensitive health data that are now shared on our phones.

While many are familiar with the Health Insurance Portability and Accountability Act (HIPAA) and will look to HIPAA for guidance, the law does not cover most of the activities that people engage in with respect to data about their health and wellness in mobile apps. Instead, the collection and sharing of these data is primarily governed by consumer protection regulations and state privacy laws such as the CPRA.

In the absence of a federal privacy law, the CPPA is positioned to be one of the most important regulators of data protection rules in the country.

1. Sensitive Personal Information

In order to create comprehensive, fair rules regarding *sensitive personal information*, it is critical to correctly define what it constitutes. Specifically, information concerning a consumer's health should be understood contextually.

One of the most encouraging developments of the CPRA is its protection of data that many users will expect to remain private and secure. The CPRA adds a category of personal information termed “sensitive personal information” (SPI). SPI includes, among other items, “personal information collected and analyzed concerning a consumer's health,” or “personal information collected and analyzed concerning a consumer's sex life or sexual orientation.”³ However, rulemaking will need to further define what is meant by personal information concerning a consumer's health.

This will be no easy task. Many health apps collect information such as hours of sleep or number of steps, which some may consider to be non-sensitive, but can, in fact, be used to make inferences about a person's physical or mental health. Often, data can be amalgamated and analyzed to make inferences that would otherwise be considered very sensitive information. For instance, data on missed periods and the user's age in a period-tracking app may suggest an individual is pregnant or approaching menopause. Furthermore, when vast amounts of data are collected about users, machine learning tools can identify patterns of behavior that would not otherwise be revealed. In addition to apps using chatbots,⁴ we found some health apps, like Premom, appear to be using machine learning tools like TensorFlow to predict ovulation cycles.

³ CA, Civ. Code, § 1798.185(a)(1).

⁴ For instance, the app [Wysa](#), which functions as a therapy chatbot, discloses the use of Kubit AI in their privacy policy.

Therefore, the CPPA should understand SPI as contextual since a rigid definition may be over- or under-inclusive in fully protecting user data privacy.

We recommend that the CPPA look to the [Consumer Privacy Framework for Health Data](#), created by the Center for Democracy & Technology (CDT) and E-Health Initiative (EHI) as a guide to further develop the definition of SPI. The Framework defines “consumer health information” as information that relates to the *analysis* of an individual’s physical or mental health. This term “rejects previous notions of ‘health data’ that are limited to the direct provision of health services by a professional” and focuses instead “on the nature of the information and how it is used.”⁵

Furthermore, a broad definition of “collection and analysis” is crucial to protect users.

As part of our investigation, we observed that many of the femtech and mental health apps collect SPI but the CPPA will need to determine a threshold regarding what constitutes the “collection *and* analysis” of consumers’ information. To ensure all data handlers are obligated to follow provisions related to SPI, the CPPA should create a low threshold for this definition, interpreting “analysis” broadly. Our research shows that there are often multiple entities that handle user data, and a narrow definition of “analysis” would leave some of these entities uncovered by the law.

The CPPA should look to comparable provisions, such as Article 4 of the General Data Protection Regulation (GDPR) and its definition of “processing,” which includes “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”⁶ By understanding analysis as analogous to “processing” as it is defined under GDPR, the CPPA will ensure users’ data is adequately protected.

2. New Consumer Rights Under the CPRA

The CPRA also establishes consumers’ rights to limit the use and disclosure of their sensitive personal information. As such, the Agency has invited comments on what rules and procedures should be established to allow consumers to limit businesses’ use of their sensitive personal information. IDAC strongly recommends the CPPA adopt rules and procedures that require companies to provide users with clear and accessible opt-out mechanisms free of dark patterns,

⁵ See page 10: “Proposed Consumer Privacy Framework for Health Data,” February 2021, <https://cdt.org/wp-content/uploads/2021/02/2021-02-09-CDT-and-eHI-Proposed-Consumer-Privacy-Framework-for-Health-Data-d-FINAL.pdf>

⁶ General Data Protection Regulation (GDPR), Art. IV. , <https://gdpr-info.eu/art-4-gdpr/>.

user interface designs that manipulate and “push people toward actions they might not have chosen otherwise,”⁷ such as consenting to questionable data collection.

Under this new provision, companies who use or disclose SPI must provide a clear and conspicuous link titled “Limit the Use of My Sensitive Personal Information.” Selecting this link will limit the disclosure of SPI to that “which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods and services.”⁸ Unfortunately, the exercising of this right is structured as an opt-out. Elsewhere, [IDAC has written](#) about how dark patterns can be used to circumvent the law’s opt-out requirements.

Based on our research, IDAC believes that stronger enforcement is necessary to ensure that app companies comply with limiting use of SPI to that which is necessary for the app to function. For example, in our examination of 50 fitness and weight loss apps, almost half (21) requested access to a users’ precise location.⁹ We also observed 14 femtech apps and six mental health apps requesting access to a user’s precise location data. The majority of these apps did not describe in detail why location data collection was necessary for the app’s functionality, often providing vague and questionable language around why such data collection is necessary.

We also encourage the CPPA to consider identifiers such as WiFi MAC addresses and IP addresses as proxies for geo-location. What constitutes location data is incredibly difficult to define; this is because when most smart devices connect to the Internet, they typically transmit information that allows apps to learn the general or specific location of that device. When this data is paired with users’ device identifiers and other personal information, an intimate profile of the user can be ascertained.

Lastly, we encourage the CPPA to increase enforcement of disclosure practices. Under the CCPA, companies’ privacy policies must list the categories of personal information collected.¹⁰ Of the 152 apps we analyzed, however, only 125 of those apps disclose that they collect personal information – and of that group, only 67 disclosed the collection of health information. When the CPRA takes effect, companies will have to provide notice at collection to consumers, disclosing the categories of Sensitive Personal Information to be collected, the purposes for which they will be used, whether this information will be sold or shared, and the length of time the business intends to retain each category of Sensitive Personal Information.¹¹

⁷ Consumer Reports, “Dark Patterns,”

<https://www.consumerreports.org/digital-rights/dark-patterns-tip-line-report-manipulative-practices-a1196931056>

⁸ CA. Civ. Code § 1798.121(a).

⁹ While there are clear use cases for the need of location data for many fitness and weight loss apps, such as to track a run or distance traveled, the need for location data must be judged on a case-by-case basis. For example, the need for location data for a calorie tracking app is not as clear.

¹⁰ CA. Civ. Code § 1798.130(a)(5).

¹¹ CA. Civ. Code § 1798.121.

3. Concerns Regarding the Widespread Use of Advertising and Analytics in Health Apps

Many apps that handle sensitive personal information are financially incentivized to share user information with third parties.

IDAC's research revealed several concerning trends regarding the prevalence of third-party data sharing with advertising and analytics companies. The current business models of many apps strongly incentivize the collection of personal data in order to sell it to third party advertisers and data brokers. In our investigation, we found 44 health apps sharing data with third parties. These apps are sold to consumers as safe, trustworthy resources for health needs; they appear in the platforms' app stores as falling under medical, health, and wellness categories of apps. They span all types of services, from mental health apps providing guidance for depression and bipolar disorders, to breastfeeding and baby health trackers. Despite the private and personal nature of this information, these apps also share users' data with companies that promise to analyze users' online behavior to show them personalized ads.

While most health apps are observing the letter of the law that they are required to follow, the rules themselves are inadequate. Law enforcement cannot directly tackle the financial incentives for sharing user data, but there is an important opportunity here to focus CPPA rulemaking on delineating what companies can and cannot do.

The Agency should continue to move past outdated notice-and-consent models and focus on creating rules that spell out what companies can and cannot do with consumer information.

Disclosure practices are important. They encourage transparency and enable law enforcement and watchdogs to ensure that companies actually abide by the promises they make. Nonetheless, disclosing data collection and third-party data sharing in dense, jargon-filled privacy policies should not give companies leeway to use consumers' highly sensitive information. Notice-and-consent regimes alone are inadequate to fully protect users because they place a disproportionate burden of protecting privacy on consumers.¹² Similarly, opt-out notices may serve as a step in the right direction for giving users more digital agency, but ultimately still place burdens on individuals to understand *how* to opt-out and *what* exactly they are opting out of.

IDAC strongly recommends that the CPPA focus its rulemaking on *data collection and use practices* that ensure data is used for limited purposes consistent with consumer expectations, placing the burden on companies to comply with those rules, rather than placing the burden on users. This is the approach that CDT & EHI take in their Framework.¹³ For instance, the CPPA

¹² Claire Park, "How 'Notice and Consent' Fails to Protect Our Privacy," New America, (Mar. 23, 2020), <https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/>

¹³ See *page 15*: "Proposed Consumer Privacy Framework for Health Data," February 2021, <https://cdt.org/wp-content/uploads/2021/02/2021-02-09-CDT-and-eHI-Proposed-Consumer-Privacy-Framework-for-Health-Data-d-FINAL.pdf>

could strengthen enforcement of data minimization and greater contractual obligations for third parties.¹⁴

The back-end data economy poses a challenge to oversight.

One of the challenges the CPPA will face is how to effectively hold actors accountable in the back-end data economy. As mentioned, Agency rulemaking can and should focus on data collection and use, but too often, data is sold and stored by multiple parties. In the mobile app marketplace, this concern is especially apparent when apps sell sensitive information like location data “unbeknownst to most users.”¹⁵ While privacy policies and in-app disclosures may truthfully describe how an app uses personal data, it can be difficult for users to discern “which apps on your phone simply use the data for their own functional purposes and which ones release your data into the economic ether.”¹⁶ These third parties often do not have any direct relationships with users¹⁷ and it is very difficult to trace where their data goes after it leaves an app.

One of the reasons for this lack of traceability is the use of software development kits, or SDK’s, which many developers use to build their applications. Sometimes even developers are unaware of the data their SDK’s collect, and with whom the SDK’s companies share information with.

Law enforcement and watchdog groups alike have little to no visibility into this practice and the policy problems it poses. But we do know from reports that in some cases, the back-end data economy is allowing questionable actors to build personality profiles built with intimate demographic data¹⁸ or buy and sell users’ location data.

¹⁴ CA. Civ. Code § 1798.100, “General Duties of Businesses that Collect Personal Information,” outlines data minimization requirements (§ 1798.100(c), “A business’ collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed”) and third party contractual obligations (§ 1798.100(d)(2), “A business that collects a consumer’s personal information and that sells that personal information to, or shares it with, a third party. . .shall enter into an agreement [that] obligates the third party [] to comply with applicable obligations under this title.”)

¹⁵ Jon Keegan and Alfred Ng, “There’s a Multibillion-Dollar Market for Your Phone’s Location Data,” The Markup (Sept. 30, 2021),

<https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data>

¹⁶ *Id.*, quoting Serge Egelman, a researcher at UC Berkeley’s International Computer Science Institute and CTO of AppCensus.

¹⁷ Norwegian Consumer Council, “Out of Control: How consumers are exploited by the online advertising industry,” (Jan. 14, 2020),

<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>

¹⁸ Sue Halpern, “How the Trump Campaign’s Mobile App Is Collecting Huge Amounts of Voter Data,” The New Yorker (Sept. 13, 2020),

<https://www.newyorker.com/news/campaign-chronicles/the-trump-campaigns-mobile-app-is-collecting-massive-amounts-of-voter-data>

4. The Role of Watchdogs


While rulemaking on these subjects is necessary and consequential, companies -- particularly those in digital spaces -- cannot be held accountable by law enforcement alone. Internet governance differs from other regulatory regimes because it is difficult for traditional notice-and-comment to move at the speed of the Internet. In addition to clearer rules for companies, there should be proactive identification of risks and harms, education to developers, resolution of problems upstream rather than just waiting until they crystalize into clear violations of law that have already harmed people. Independent privacy watchdogs can identify risks to consumers that are difficult for traditional law enforcement agencies to police. Watchdogs can also play a crucial role in educating developers and companies, so these harms never manifest in the first place.

As IDAC has written previously, our model encompasses a three-pronged approach, with (1) clear rules developed with stakeholders, (2) comprehensive training for practitioners, and (3) robust, proactive, and credible accountability measures to ensure compliance with applicable rules.¹⁹ When these efforts coincide, there will then be an ecosystem that individuals can trust.

5. Conclusion

We appreciate the opportunity to submit comments on proposed rulemaking under the California Privacy Rights Act of 2020. Please do not hesitate to contact us with any questions.

Sincerely,

Ginny Kozemczak
Chief of Staff & Policy Counsel

International Digital Accountability Council

¹⁹ IDAC, “Rebuilding Trust in the Digital Ecosystem: New Mechanisms for Accountability,” (Mar. 10, 2021), <https://www.gmfus.org/news/rebuilding-trust-digital-ecosystem-new-mechanisms-accountability>

From: Tonsager, Lindsey [REDACTED]
Sent: 11/8/2021 6:25:13 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Scott, Alexandra [REDACTED]
Subject: PRO 01-21 - Preliminary Comments of the Entertainment Software Association
Attachments: ESA - CPRA Rulemaking Comments.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Dear Ms. Castanon:

Please find attached the Entertainment Software Association's preliminary comments on the proposed rulemaking under the California Privacy Rights Act.

Respectfully submitted,
Lindsey Tonsager
Counsel for the Entertainment Software Association

Lindsey Tonsager
Pronouns: She/Her/Hers

Covington & Burling LLP
Salesforce Tower, 415 Mission Street, Suite 5400
San Francisco, CA 94105-2533

www.cov.com

COVINGTON

This message is from a law firm and may contain information that is confidential or legally privileged. If you are not the intended recipient, please immediately advise the sender by reply e-mail that this message has been inadvertently transmitted to you and delete this e-mail from your system. Thank you for your cooperation.



November 8, 2021

Via Email

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

RE: Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2021 (PRO 01-21)

Dear Ms. Castanon:

The Entertainment Software Association ("ESA")¹ submits these comments in connection with the California Privacy Protection Agency's ("CPPA") preliminary efforts to implement regulations under the California Privacy Rights Act ("CPRA").²

ESA respectfully requests that the CPPA adopt regulations that:

- Discourage fraudsters and other bad actors from attempting to use the correction right to undermine the security or integrity of the service or facilitate their unlawful or malicious conduct.
- Ensure that any technical specifications for the voluntary opt-out preference signal are consistent with existing children's privacy laws and reliably convey a parent's or user's choice.
- Provide consumers meaningful access to personal information, while maintaining the safety, security, and integrity of the business's services.
- Clarify what constitutes "dark patterns" and "precise geolocation" information to align with the Federal Trade Commission's precedent and guidance.
- Consistent with the statutory text, specify that consumers can opt out of automated decisionmaking only where such data processing uses or discloses sensitive personal information, and ensure that disclosing meaningful information about the logic of such data

¹ ESA is the U.S. association for companies that publish computer and video games for video game consoles, handheld devices, personal computers, and the internet. There are over 400 video game companies in the state of California.

² California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Sept. 22, 2021), https://coppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

processing does not adversely impact intellectual property rights or efforts to detect and prevent fraud or other malicious conduct.

We explain each of these requests in more detail below.

I. The regulations should discourage fraudsters and other bad actors from attempting to use the correction right to undermine the security or integrity of the service or facilitate their unlawful or malicious conduct.

In the experience of ESA's members, fraudsters and other bad actors can abuse correction rights to try to evade detection, gain unauthorized access to an account, or otherwise facilitate their unlawful or malicious conduct. For example, a video game player who has been banned from an online game for harassing other players or cheating in violation of the game's terms of use might attempt to request "correction" of their IP address, username, or other personal information in order to try to circumvent the game company's anti-fraud, anti-cheat, and other detection systems that prevent such players from attempting to create new accounts. Malicious actors also may try to use the "correction" right to try to make it easier to gain unauthorized access to another user's account or regain access to a fraudulent account. To discourage such efforts, the regulations should make clear that where a business has a reasonable belief that the particular consumer is attempting to abuse the correction right for malicious purposes, it may deny correction requests in order to prevent fraud, including requests that would undermine the security or integrity of the service or facilitate unlawful or otherwise malicious conduct.

Specifically, ESA requests that the CPPA include the following in its CPRA regulations:

Nothing in these regulations shall restrict a business's, service provider's, third party's, or contractor's ability to: prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive conduct, or any unlawful activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action.³

Such language is necessary to maintain consistency with the plain text and clear intent of the CPRA, which allows businesses to deny requests that are not "verifiable" and also recognizes the need to balance the rights of consumers with the need to protect others and discourage unlawful activity.⁴ It

³ This language is consistent with other state laws that empower businesses to protect consumers from fraudulent and malicious conduct. *See, e.g.*, Virginia Consumer Data Protection Act 59.1-578(A)(7); Colorado Privacy Act 6-1-1304(3)(A)(X).

⁴ *See, e.g.*, CPRA §§ 1798.106(c) (requiring businesses to correct personal information in response to a verifiable consumer request only); 1798.185(a)(8)(C) (balancing the correction right against the need to prevent fraud); 1798.185(a)(8)(B) (balancing the correction right against the need for accuracy); 1798.145(a)(3) (recognizing that the correction right does not restrict a business's ability to cooperate with law enforcement agencies regarding conduct that the business has a good faith belief is illegal); 1798.145(a)(5) (preventing correction where it would limit a business's ability to exercise or defend against legal claims); 1798.145(k) (recognizing that the correction right should not adversely affect the rights and freedoms of others); 1798.140(ac) (recognizing the need to protect system "security and integrity").

also is supported by the existing text of the California Consumer Privacy Act (“CCPA”) regulations and the commentary that the California Attorney General published when issuing those regulations.⁵

II. The regulations should ensure that any technical specifications for a voluntary opt-out preference signal are consistent with existing children’s privacy laws and reliably convey a parent’s or user’s choice.

The CPRA’s voluntary opt-out preference signal has the potential to provide an innovative new mechanism for consumers to exercise their CPRA rights and for businesses to have flexibility in how they choose to provide notice about and respond to consumers’ opt-out requests. However, whether this mechanism succeeds or fails depends in large part on whether it proves reliable in accurately conveying the person’s intended choice and avoids conflicting with other consent mechanisms.

Ensuring reliability and avoiding conflicting consent mechanisms is especially critical with respect to consumers who are under the age of 13, because any technical specifications for a voluntary opt-out preference signal must be carefully designed to ensure consistency with the Children’s Online Privacy Protection Act (“COPPA”). Any business whose online service is directed to children under 13 or that has actual knowledge that it collects personal information online from California consumers younger than 13 years of age must also comply with COPPA. COPPA preempts any action by a state or local government that imposes “any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in [COPPA] that is inconsistent with the treatment of those activities or actions under [COPPA].”⁶

To ensure consistency with COPPA, the CPRA regulations must require businesses to honor any preference signal for children under 13 years old only if such signal satisfies COPPA’s standard for

⁵ See, e.g., Cal. Code Regs. Tit. 11, §§ 999.314(c)(4) (permitting service providers to use personal information for security and anti-fraud purposes); 999.315(g) (allowing a business to refuse fraudulent opt-out requests); 999.323(c) (authorizing the collection of additional information during the verification process for security and fraud-prevention purposes); California Department of Justice, Initial Statement of Reasons, at 29, <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf> [hereafter, “ISOR”] (noting that the regulations require “a business to consider a variety of factors in determining the verification method, such as . . . the likelihood that fraudulent or malicious actors are seeking the information”); ISOR, 31 (explaining that the regulations “provide clear direction that the business should prioritize security and fraud-prevention over disclosure”); California Department of Justice, Final Statement of Reasons, at 19, <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf> [hereafter, “FSOR”] (explaining that the verification process is for “minimizing the risk of fraud or malicious activity”); FSOR, 34 (explaining that the regulations permit service providers to use personal information “to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity”); FSOR, Appendix A, Row 744, <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf> [hereafter “Appendix A”] (explaining that the regulations require “businesses to not comply with a consumer’s request if it suspects fraudulent or malicious activity”); ISOR, 44 (“Given the wide variety of different industries subject to the CCPA, prescribing a particular method of verification may not provide the flexibility necessary to address all the different circumstances in which businesses and consumers interact, nor would it address changing data security standards and evolving technologies.”).

⁶ 15 U.S.C. § 6502(d).

“verifiable parental consent.” Under COPPA, parents must provide “verifiable parental consent” before a business may collect, use, or disclose online the personal information of children under 13 years old, unless one of COPPA’s various exceptions applies.⁷ Importantly, COPPA requires that the parent’s choices be “verifiable,” and the COPPA statute and more than a decade of Federal Trade Commission guidance make clear that the standard is a high bar for ensuring that it is the child’s parent or legal guardian who is exercising the choice.⁸ Consequently, to ensure consistency with COPPA, the CPRA regulations must not require a business whose online service is child-directed or that has actual knowledge that it collects personal information from a child under the age of 13 to respond to the preference signal unless the signal constitutes “verifiable parental consent” as that term is defined in COPPA.

In addition, the CPRA regulations must not require businesses to honor any preference signal for children under 13 years old from an authorized agent of a parent or legal guardian. Under COPPA, only parents and legal guardians may exercise the right to consent (or withdraw consent) for the online collection, use, or disclosure of their child’s personal information.⁹ Consequently, the CPRA regulations must not require a business whose online service is child-directed or that has actual knowledge that it collects personal information from a child under the age of 13 to respond to a preference signal from any authorized agent who does not appear to be the parent or legal guardian of the child.

The invitation for preliminary comment also specifically asks “what technical specifications should be established for an opt-out preference signal that allows the consumer, or the consumer’s parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.”¹⁰ Because any technical specification that signals age would contradict clear, long-established Federal Trade Commission (“FTC”) guidance and ultimately is likely to prove too unreliable to effectively promote the CPRA’s goals, ESA requests that the CPRA regulations not include any such technical specification. The FTC has long held that websites and online services that are primarily directed to children under 13 must presume that all users are under the age of 13 and cannot

⁷ *Id.* § 6502(a); 16 C.F.R. § 312.5.

⁸ *See, e.g.*, ISOR, 34 (“The requirement of a ‘reasonable method’ is based on the similar requirement in the Children’s Online Privacy Protection Act (hereinafter COPPA) (15 U.S.C. § 6501, et seq.). . . . The methods are the same as those set forth in regulations issued by the Federal Trade Commission in furtherance of COPPA[.]”); Appendix A, Row 798 (“Section 999.330(a)(2) has been modified to clarify that acceptable methods are not limited to the ones listed in the regulations.”); 15 U.S.C. §§ 6501(9), 6502(b); 16 C.F.R. § 312.5.

⁹ 16 C.F.R. § 312.2 (defining “parent” to include a legal guardian); 15 U.S.C. § 6501(9) (defining “verifiable parental consent” to be “any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that **a parent of a child** receives notice of the operator’s personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.”)(emphasis added).

¹⁰ CPRA, *supra* note 2, at 4.

age gate.¹¹ The proposal would appear to conflict with this approach by allowing business that operate primarily child-directed sites or services to rely on the purported age conveyed through the preference signal to determine whether a parent or the child can exercise the applicable rights over use or disclosure of personal information. The proposal also would appear to conflict with the FTC's guidance on age screens.¹² Families often use shared devices across a household, particularly in the context of video gaming. For example, a parent may install a video game on their mobile phone, tablet, or personal computer and then hand that device over to their child to play. If an adult previously set a preference signal for that device, that default would presumably continue to apply even though COPPA requires neutral age screen mechanisms without defaults. If the preference signal was changed to indicate that the user is under 13 and is subsequently changed back to indicate an older age, it would be impossible to know whether that change was done by the parent or the child. Such a result is inconsistent with the FTC's guidance, which recommends using technical means "to prevent children from back-buttoning to enter a different age."¹³

Because purported age information delivered via preference signal is likely to be so unreliable, it creates a significant risk that companies will receive conflicting age information from the user or their parent or guardian. Importantly, the FTC has repeatedly reiterated that businesses (including, but not limited to, general audience sites) have no duty to investigate age,¹⁴ so any regulations that would, in effect, create such a duty to resolve conflicts between the age a user or their parent or guardian provides during account creation and the age indicated through the preference signal (which could potentially change repeatedly over time and as described above, would not be reliable evidence of a user's actual age) would be inconsistent with COPPA.¹⁵ For example, when a parent creates an account for their child with the provider of a video game console or a video game publisher, they may provide the child's date of birth and (if that child is under 13) grant verifiable parental consent consistent with COPPA to the requested online collection, use, and disclosure of the child's personal information. If that child is subsequently playing the game but conflicting age information is provided through the preference signal, this conflict makes the business's obligations under the CPRA unclear. It is also not clear how a parent or legal guardian could exercise different opt-out preferences if they have multiple children under 13 years of age, or how different preferences could be communicated for these young children, the parents themselves, and other children in the household who might be at least 13 years of age, absent the collection of more personal information than may otherwise be needed to provide the

¹¹ See, e.g., FTC, *Complying with COPPA: Frequently Asked Questions*, at H.2 (July 2020) [hereinafter "COPPA FAQ"], available at <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0>.

¹² See *id.* at D.7.

¹³ *Id.*

¹⁴ See, e.g., COPPA FAQ, at E.2; 76 Fed. Reg. 59804, 59806 (stating that operators need not "ferret through a host of circumstantial information to determine who may or may not be a child").

¹⁵ Notably, the FTC previously has encouraged the development of a technical specification to allow operators of child-directed sites and services to signal their status to third parties (such as social media plug-ins and ad networks) to facilitate COPPA compliance. Unlike such a signal, which can convey a static, reliable fact (i.e., that the particular website address is child-directed), purported age information (which varies over time and across individuals) cannot be reliably and effectively conveyed using a preference signal.

requested services. Such a fundamental paradigm shift away from a free and open internet with room for anonymous speech to an identity-based internet requiring verification for all online activity does not appear to have been contemplated or intended under the CPRA.

III. The regulations should require businesses to provide consumers with meaningful information while also permitting them to maintain the safety, security, and integrity of their services and systems.

The regulations should carefully balance the need to provide consumers meaningful access to the personal information they provide and the need to maintain the safety, security, and integrity of the service and systems.

Specifically, video game companies should not be obligated to return system logs, technical gameplay data, and similar technical data in response to a consumer's access request. As a threshold matter, this data generally is not personal information. Moreover, the CPRA specifies that businesses must provide only the "specific pieces of personal information obtained from the consumer" in response to access requests.¹⁶ The text "from" is plain that only personal information that the consumer provides directly is subject to this access right. System logs, technical gameplay data, and similar technical data is automatically generated by the business, and is not "from" the consumer. Such data also often includes trade secrets,¹⁷ and malicious actors may be able to use it to undermine a business's efforts to detect and prevent security incidents, cheating, fraud, and other unlawful or malicious activity.¹⁸

For these reasons, ESA respectfully requests that the CPPA include the following provision in its regulations:

Nothing in these regulations shall require businesses to provide consumers with access to system logs and similar technical data,

¹⁶ CPRA § 1798.130(a)(3)(B)(iii).

¹⁷ *Id.* at § 1798.185(a)(3) (requiring regulations to establish "any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter, with the intention that trade secrets should not be disclosed in response to a verifiable consumer request").

¹⁸ *Id.* at §§ 1798.130(a)(3)(B)(iii) (specifying that "'specific pieces of information' do not include data generated to help ensure security and integrity"); 1798.140(ac) (defining "security and integrity" as "the ability: (1) of a network or an information system to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information; (2) to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions, and to help prosecute those responsible for such actions; and (3) a business to ensure the physical safety of natural persons"); *see also* Cal. Code Regs. Tit. 11 § 999.313(c)(4) ("A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics.").

*automatically generated data, or any data used for security and integrity purposes.*¹⁹

IV. The regulations clarifying “dark patterns” should align with the Federal Trade Commission’s longstanding precedent and guidance on unfair or deceptive practices.

The CPRA’s current “dark patterns” definition, which determines when a user’s consent is effective for purposes of the CPRA, is vague. Accordingly, the CPPA should clarify in its regulations what consent practices constitute dark patterns by incorporating and aligning with existing FTC precedent and guidance. The CPRA defines dark patterns as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.”²⁰ This definition creates ambiguity because key concepts—such as “substantial,” “subversion,” and “autonomy”—are nebulous. The definition’s vagueness potentially chills constitutionally-protected commercial speech, since such speech is designed to affect individuals’ decisionmaking.

The ESA therefore urges the CPPA to enact regulations that clarify the CPRA’s “dark patterns” definition by incorporating and aligning with the FTC’s robust taxonomy of user interface designs that the FTC has deemed are unlawful as unfair or deceptive practices. Over the last forty years, the FTC has issued various guidance on unlawful disclosure and design practices and enforced against companies that sought to deceive consumers through such practices. As illustrated throughout its prior enforcement actions and guidance, the FTC has identified the following practices as unlawful: (1) buried language that obscures material disclosures in terms;²¹ (2) poorly-labeled hyperlinks that hide material terms from consumers;²² (3) trick language that confuses consumers;²³ and (4) bait and switch practices.²⁴ The CPPA should clarify the CPRA’s definition by specifying that these practices constitute

¹⁹ CPRA § 1798.130(a)(3)(B)(iii) (specifying that the specific pieces of information that must be provided in response to an access request do not include “data generated to help ensure security and integrity or as prescribed by regulation”).

²⁰ CPRA § 1798.140(l).

²¹ FTC, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising*, at 10, 18 (2013) [hereinafter “*.com Disclosures Guidance*”].

²² See, e.g., *id.* at ii (explaining that hyperlinks should provide access to disclosures that are not integral to the claim and should be labeled in a way that conveys the type and import of information to which they lead if clicked); Complaint, *FTC v. Vizio, Inc.* (Feb. 6, 2017) (“The notification provided no information about the collection of viewing data or ACR software. Nor did it directly link to the settings menu or privacy policy.”).

²³ See, e.g., *.com Disclosures Guidance*, at Appendix (detailing twenty-two examples of clear and unclear disclosures); Press Release, *Rent-To-Own Payment Plan Company Progressive Leasing Will Pay \$175 Million to Settle FTC Charges It Deceived Consumers About Pricing* (2020); Complaint, *In re Facebook Inc.* (Aug. 10, 2012); Complaint, *In re PayPal, Inc.* (May 24, 2018).

²⁴ See, e.g., FTC, *Advertising FAQ’s: A Guide for Small Business* (2001); *Guides Against Bait Advertising*, 16 C.F.R. § 238.0 (2012); Press Release, *Abating Bait-and-Switch Buyback Tactics for Devices* (2016); Press Release, *The Lead-Generation Bait-and-Switch* (2019); FTC, *Native Advertising: A Guide for Businesses* (2015).

dark patterns and that therefore consent is not effective under the CPRA when businesses obtain consent using such unlawful practices.²⁵

V. The regulations to further define precise geolocation should be informed by the FTC’s guidance.

Any regulations that further define precise geolocation information should be consistent with and informed by how the FTC has defined and interpreted that term in its guidance and prior enforcement actions.

The CPRA currently defines precise geolocation as “any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.”²⁶ The CPRA also recognizes that personal information that reveals “precise geolocation” is a type of sensitive personal information, thereby giving consumers the right to limit its use and disclosure in certain circumstances.²⁷

While the FTC similarly has interpreted precise geolocation information to be data that is derived from a device (based, for example, on GPS, WiFi, or cell-tower data), the FTC has not imposed any arbitrary geographic radius based on this location. Because the proposed definition of “precise geolocation” is inconsistent with how that term has been interpreted and applied by the FTC, it could create consumer confusion regarding the scope or meaning of privacy settings or representations related to precise geolocation information.²⁸ Accordingly, ESA respectfully requests that the CPPA adopt the following language in its final regulations to align with the FTC’s definitions of precise geolocation information:

“Precise geolocation” means any data that is derived from a device (including GPS, WiFi, or cell tower) and that (1) is used or intended to be used to locate a consumer and (2) is sufficient to identify street name and name of city or town.

²⁵ CPRA §§ 1798.140 (specifying that “agreement obtained through use of dark patterns does not constitute consent”); 1798.185(20) (specifying that links to a webpage or supporting content “that allows the consumer to consent to opt-in [shall not] make use of any dark patterns”).

²⁶ CPRA § 1798.140(w).

²⁷ *Id.* at §§ 1798.140(ae)(1)(C), 1798.121.

²⁸ COPPA FAQ, at G.3 (“The Rule covers ‘geolocation information sufficient to identify street name and name of city or town.’”); *see also* Decision and Order, *In re* Goldenshores Technologies LLC (F.T.C. Mar. 31, 2014), available at <https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf> (“precise geolocation data of an individual or mobile device, including but not limited to GPS-based, WiFi-based, or cell-based location information”); Decision and Order, *In re* Uber Technologies Inc. (F.T.C. Oct. 25, 2018), available at https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf; Stipulated Order for Permanent Injunction and Civil Penalty Judgment (same).

VI. Any opt-outs with respect to automated decisionmaking technologies should align with the statutory text as well as efforts to protect the safety of consumers and intellectual property rights.

Consistent with the CPRA's text, the regulations should provide consumers with the ability to opt out of automated decisionmaking technology that uses or discloses sensitive personal information. Additionally, the regulations should balance giving consumers access to information about automated decisionmaking technology with the need to protect consumer safety and intellectual property rights.

A. *The regulations should permit consumers to opt out of automated decisionmaking technology that uses or discloses sensitive personal information.*

The CPRA expanded the scope of the CCPA to provide consumers specific new opt-out rights—namely to opt out of the sharing of personal information for cross-context behavioral advertising and the right to opt out of certain uses and disclosures of sensitive personal information.²⁹ Notably, the statute did *not* create a blanket right to opt out of all automated decisionmaking technologies.³⁰ Accordingly, the CPPA's authority to issue regulations related to automated decisionmaking opt-outs is limited to interpreting the scope and application of the existing statutory opt-out rights.

The consumer opt-out right that most closely relates to automated decisionmaking technology is the right to limit the use and disclosure of sensitive personal information. Significantly, automated decisionmaking technology includes “profiling,” which is defined to include sensitive processing concerning the consumer’s work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.³¹ This interpretation is further supported by the fact that these “profiling” activities generally track the types of personal information that are “sensitive” under the CPRA, including union membership (a type of information concerning work performance); financial account information (concerning the consumer’s economic situation); genetic and health data (concerning the consumer’s health); personal preferences and interests data (concerning the consumer’s religious or philosophical beliefs), behavioral data (concerning sex life), and precise geolocation (concerning a consumer’s location or movements).³² Accordingly, ESA respectfully requests that the CPPA adopt regulations that state the following:³³

²⁹ CPRA §§ 1798.120 (opt-out of sharing); 1798.121 (limit the use and disclosure of sensitive personal information).

³⁰ Appendix A, Row 17 (“The OAG cannot implement regulations that alter or amend a statute or enlarge or impair its scope.”); *see also People v. K.P.*, 30 Cal. App. 5th 331, 341, 241 Cal. Rptr. 3d 324, 331 (2018) (“The failure of the Legislature to change the law in a particular respect when the subject is generally before it and changes in other respects are made is indicative of an intent to leave the law as it stands in the aspects not amended.”) (internal quotations omitted).

³¹ CPRA § 1798.140(z).

³² *Id.* § 1798.140(ae).

³³ In addition, the CPRA's blanket statutory exemptions would apply with respect to this right as well. *See, e.g.*, CPRA § 1798.145.

A consumer may request to opt out of a business's use of automated decisionmaking technology to the extent such technology uses or discloses the consumer's sensitive personal information.

In addition to ensuring that the regulations are consistent with the text and purpose of the CPRA statute, the above approach also harmonizes the CPRA with international standards governing automated decisionmaking technologies. For example, Article 22 of the EU General Data Protection Regulation provides individuals the right to avoid being subject to automated decisionmaking, including profiling, where it “produces legal effects concerning him or her or similarly significantly affects him or her.”³⁴ Interpreting the CPRA’s automated decisionmaking opt out to apply to the extent such technology uses or discloses the consumer’s sensitive personal information would result in similarly scoping this right to automated decisions that are likely to produce legal or similarly significant effects.

B. Disclosures of meaningful information about automated decisionmaking logic should be consistent with the statutory text and not adversely impact intellectual property rights or efforts to combat malicious conduct.

We support the CPRA’s goal of providing consumers meaningful information about the logic used for automated decisionmaking technologies. As explained above, however, such rights should be aligned with the statutory text’s focus on automated decisionmaking technologies that use or disclose sensitive personal information and therefore risk having a legal or similarly significant effect on the consumer. Moreover, the CPRA regulations should provide businesses flexibility to disclose meaningful information to consumers, while balancing the need to protect intellectual property rights and to prevent fraud and other malicious conduct. Depending on the sensitivity of the automated decisionmaking process and the types of personal information used, this could include, for example, providing a general explanation of how the automated decisionmaking process functions, the purposes for which such process is used, and the types of data or sources of personal data such process uses. The California Attorney General adopted a similar approach when that office issued regulations requiring privacy policies to include only a “general description” of verification processes. The California Attorney General explicitly recognized that businesses should not have to provide bad actors with a blueprint to evade their verification processes.³⁵

Accordingly, ESA respectfully requests that the CPPA include the following language in the CPRA regulations:

A consumer may request to receive meaningful information about the logic of automated decisionmaking technology that uses or discloses the consumer's sensitive personal information. In responding to such a

³⁴ Regulation (EU) 2016/679 (Apr. 27, 2016).

³⁵ Appendix A, Row 375 (“Section 999.313(a) has been modified to only require a business to disclose a general description of the business’s verification process. A general description of the verification process would not raise any security or fraud concerns while still informing consumers’ expectations regarding the response process.”).

request, a business shall be required to disclose a general description of its automated decisionmaking processes.³⁶

* * *

ESA appreciates the CPPA's consideration of these comments, and we look forward to continuing to work with the CPPA on these important issues.

Sincerely,



Gina Vetere
Senior Vice President and General Counsel
Entertainment Software Association

³⁶ This language aligns with the CCPA. Cal. Civ. Code § 1798.110(b) ("A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer."); Cal. Code Regs. Tit. 11, §§ 999.308(c)(1)(c), (2)(c) (requiring privacy policies to include the following information about deletion and access requests: a "[g]eneral description of the process the business will use to verify the consumer request, including any information the consumer must provide.").

From: Michelle De Mooy [REDACTED]
Sent: 11/8/2021 4:50:34 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: MPA The Association for Magazine Media Comments on Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020
Attachments: MPA The Association of Magazine Media Comments to the CPPA_Nov 8 2021.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Hello,

Attached please find MAP The Association for Magazine Media's comments on the Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020.

Thank you for the opportunity to comment and please do not hesitate to reach out if we can be helpful.
Michelle

Michelle De Mooy
Senior Director of Policy
[MPA The Association of Magazine Media](#)
[REDACTED]



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@coppa.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 Turing 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
Senior Vice President, Legislative and Regulatory Policy

From: Dylan Hoffman [REDACTED]
Sent: 11/8/2021 12:26:04 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Alexandra McLeod [alexandra@internetassociation.org]
Subject: PRO 01-21
Attachments: 11.8.21 FINAL IA Comments_CPRA CPPA Preliminary Rulemaking.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Hi,

Please find attached comments from Internet Association on Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act (Proceeding No. 01-21). Please let me know if you have any questions.

Best,

--



Dylan Hoffman

Director of California Government Affairs
[REDACTED]

INTERNET ASSOCIATION

1303 J Street, Suite 400, Sacramento, CA 95814



November 8, 2021

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

Re: Internet Association Comments on California's Privacy Protection Agency's Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act (Proceeding No. 01-21)

Dear Ms. Castanon:

Internet Association ("IA") appreciates the opportunity to provide the California Privacy Protection Agency ("CPPA/the Agency") feedback on its Preliminary Rulemaking Information Inquiry under the California Privacy Rights Act ("CPRA"). IA is the only trade association that exclusively represents leading global internet companies on matters of public policy. Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. We believe the internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, IA works to ensure legislators, consumers, and other stakeholders understand these benefits.

IA members know trust is fundamental to their relationships with consumers. Our companies recognize that to be successful they must meet consumers' reasonable expectations about how companies collect, use, and share personal information. IA members are committed to providing consumers with strong privacy protections and control over their personal information and advocate for a modern privacy framework in the IA Privacy Principles.¹ IA supports consumer privacy laws that ensure consumers have important choice and control over their personal information and businesses have clear and consistent guidance on complying with the law.

IA members support many of the privacy concepts within CPRA, such as a robust compilation of consumer rights like access, correction, deletion, transparency, and consumer choice, and we would encourage the CPPA to take a common-sense approach when interpreting provisions within the statute and create regulations that are consistent with existing and recently enacted privacy laws such as Virginia's Consumer Data Protection Act ("VCDPA"). This will allow consumers to have consistent privacy expectations across state lines and allow for businesses to comply with clear and dependable guidelines for consumer privacy protections.

¹ IA Privacy Principles for a Modern National Regulatory Framework, available at: https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/ (last accessed November 8, 2021).



Topic I: Processing that Presents a “Significant Risk to Consumers’ Privacy or Security” & Cybersecurity Audits and Risk Assessments Performed by Businesses

As noted above, IA members recommend the CPPA create uniformity across state lines by coordinating its regulations and the requirements with those of other state privacy laws like VCDPA and Colorado’s Privacy Act (“CPA”) that also become effective in 2023. As such, IA suggests aligning any data protection assessments with those requirements in the VCDPA and CPA.² These assessments focus on key issues such as the sale of personal information; the use of personal information in the context of targeted advertising for profiling if the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful impact, financial or physical injury, physical or other intrusion upon the solitude or seclusion, or private affairs or concerns that would be offensive to a reasonable person, or other substantial injury, to the consumer; processing sensitive personal information; and processing activities that present a heightened risk of harm to consumers.³ Additionally, the assessment approach within these privacy laws also provides businesses with the flexibility and ability to determine what is considered a “significant risk” to consumers based on their particular products or services. The standard for data protection assessments and cybersecurity audits should be consistent across state lines and provide clear guidelines to enable businesses to continue to innovate and build robust systems to protect consumers’ information and properly assess and mitigate their security risks.

A. When a business’s processing of personal information presents “a significant risk to consumers’ privacy or security”.

IA recommends that the Agency take the opportunity in its regulations to clearly define “a significant risk to consumers’ privacy or security.” When deciding how to define this phrase IA members ask that you consider the following limitations. In the security risk context a “significant risk” should be limited to the processing of data that, if compromised, results in an actual concrete harm to consumers. In the privacy context we suggest a “significant risk” should be limited to those acts where the processing of a consumer’s information leads to decisions that have a “legal or similarly significant effect”⁴ on a consumer.

In both the privacy and security contexts, any processing of personal information to comply with a legal obligation should be exempted from any data or cybersecurity risk assessment. This type of processing is critical to keep consumers safe and prevent bad actors from gaining access to IA companies’ internal systems. The Agency should want to encourage business participation when preventing fraud, detecting

² S.B. 1392 (“VCDPA”) § 59.1-576 (2021); C.R.S. (“CPA”) § 6-1-1309 (2021).

³ *Id.*

⁴ S.B. 1392 § 59.1-571 “Decisions that produce legal or similarly significant effects concerning a consumer” means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.”; C.R.S. § 6-1-1303 (10) “Decisions that produce legal or similarly significant effects concerning a consumer means a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.”



money laundering activities or screening for child sexual abuse materials. Thus, exempting these types of processing activities is in the best interest of all California citizens. Additionally, any personal information (including sensitive personal information) processed in the employment or human resources (HR) context⁵ should also not be categorized as information that poses a “significant risk” to consumers privacy or security for the purposes of the CPRA, and, as such, should not be subject to regular data protection or cybersecurity audits. Oftentimes, businesses are required to keep this information to comply with existing state and federal laws and subjecting the information to further scrutiny and assessment requirements would present an unnecessary burden on businesses.

B. What businesses that perform annual cybersecurity audits should be required to do, including what they should cover in their audits and what processes are needed to ensure that audits are “thorough and independent.”

IA member companies are supportive of using reasonable precautions to protect personal information from becoming lost, misused, illegally accessed, disclosed, modified or destroyed. Many IA member companies have already implemented self-assessment mechanisms to ensure their consumers’ personal information is adequately protected. These assessments include using industry standards to perform internal reviews and consistently re-certifying their systems under frameworks like ISO 27001⁶ and SOC 2⁷ to ensure that they have the necessary security processes, policies, and technological designs to protect consumer’s personal information. Therefore, as the Agency is deciding what components of a cybersecurity audit are necessary to ensure that it is “thorough and independent”, IA members would encourage the Agency to not require a third-party auditor, due to the many self-imposed mechanisms companies are already implementing to maintain and improve the security of consumers’ personal information. Instead, we would ask that the Agency consider reusing existing self-audit and certification frameworks to ensure that companies subject to the CPRA are considered already in compliance with the law as opposed to creating duplicative or onerous requirements to assess a company’s security measures.

IA members make continual improvements to ensure that consumers’ information is more secure by using cloud computing services, data minimization practices, and regular self-assessments of the information they collect, use, and store. Practices such as these should be recognized when the Agency decides what requirements are critical for conducting effective privacy and security assessments. The Agency should also look at the company’s business practices such as implementing encrypted data measures; having a data breach and recovery protocol; and the level of security monitoring the business performs. These are all elements that IA members have spent years working on and invest time and effort in to ensure the best consumer experience, but also to ensure that their consumers’ information is adequately protected.

⁵ See Cal. Civ. Code § 1798.145(m)(1).

⁶ ISO/IEC 27001 Information Security Management, ISO, <https://www.iso.org/isoiec-27001-information-security.html> (last visited November 8, 2021).

⁷ SOC 2® - SOC for Service Organizations - Trust Services Criteria, AICPA, <https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report>, (last visited November 8, 2021).



C. What businesses that submit risk assessments to the Agency should be required to do, including what they should cover in their risk assessments, how often they should submit risk assessments, and how they should weigh the risks and benefits of processing consumers' personal information and sensitive personal information.

We would again ask that any privacy risk or protection assessment requirements the Agency enacts align with the Virginia or Colorado data protection assessments⁸ and existing requirements under the General Data Protection Regulation ("GDPR"). These assessments should focus on the most significant privacy risk associated with the service or product (which could vary by company) and the actions taken to mitigate those risks such as de-identifying personal information. There is not a one-size-fits-all for a privacy assessment, but the Virginia and Colorado privacy laws outline several categories including information used for targeted advertising for profiling if the profiling presents a reasonably foreseeable risk and processing sensitive personal information as activities that should be considered in a privacy protection assessment.⁹ If the Agency were to adopt a similar structure for a privacy assessment or accept assessments that comply with other comprehensive consumer privacy laws, then businesses, including IA members, would be able to focus their attention on a unified, thorough privacy assessment process. Without this alignment among jurisdictions, businesses will have to divide resources among at least two different privacy assessment models to comply with Virginia, Colorado, and the regime this Agency presents. Lack of harmonization among the jurisdictions that require privacy risk assessments would also pose additional operational challenges for businesses.

IA would also ask that these privacy assessments occur on a "regular basis", but no more often than annually. The Agency should not require privacy assessments for activities that do not create a heightened risk as defined in VCDPA and CPA and should create a reasonable standard cadence of review for those processes that present an increased risk to consumers.¹⁰

When balancing the benefit to consumers with the costs associated with privacy assessments, again we ask that only high-risk processing activities be included in the privacy assessment. These include activities that process for targeted advertising, profile where there is a reasonably foreseeable risk of unlawful or disparate treatment, sale of data, or process sensitive information as opposed to all processing activities performed by the business.¹¹ This differentiation will allow for specific assessments to correct or evaluate behavior, such as unlawful or disparate treatment, that may need to be redirected or eliminated.

Finally, any privacy risk assessments should be used to incentivize companies to ensure comprehensive analysis and review of their processing practices-- not as a litigation defense mechanism but in order to encourage positive and productive uses of consumers' personal information. To do so, IA members would ask the Agency not to require that trade secrets or proprietary information be a part of these assessments

⁸ S.B. 1392 § 59.1-576 (2021); C.R.S. § 6-1-1309 (2021).

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*



and that all risk assessments submitted to the Agency are not able to be publicly inspected and maintain attorney-client and work-product privileges. By adopting these requests the Agency will receive a more robust assessment of the businesses' privacy processes and be empowered to better evaluate the situation at hand.

D. 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.

As the Agency considers guidance for privacy assessments it should encourage balancing the privacy risks to a consumer’s personal information against the benefit of the processing itself. During this balancing the Agency can look to factors like (1) technical safeguards put in place by the business to prevent or mitigate the risk; (2) the reasonable expectations of consumers; and (3) the processing performed in the context of the relationship between the consumer and the business. IA would recommend referencing the GDPR’s legitimate interest assessment when evaluating the risks and benefits to consumers and that the Agency should adopt or accept adequacy decisions made under the GDPR.¹²

Topic II: Automated Decision-making

IA would strongly encourage the Agency to consider that when voters passed the CPRA ballot initiative, which created the CPPA and overhauled consumers' privacy rights -- they granted limited rulemaking authority for automated decision-making technology. The voters direct this Agency to issue “regulations governing access and opt-out rights with respect to businesses’ use of automated decision-making technology ...[and] businesses’ response to access requests.”¹³ In order to align the CPPA’s regulations with the will of the voters we believe the agency’s promulgation of rules in this area should be limited.

A. What activities should be deemed to constitute “automated decision-making technology” and/or “profiling.”

Automated decision-making technology is not a universally defined term and could encompass a wide range of technology that has been broadly used for many decades, including spreadsheets and nearly all forms of software. We caution against overly broad regulation and categorizing of technology that would impede the use of socially beneficial, low-risk, and widely accepted tools, to the significant detriment of both California consumers and businesses. In fact, the California legislature encountered this problem when evaluating AB 13.¹⁴ The automated decision-making definition in this bill included everyday technology from the simplest spreadsheet to the most complex algorithm being categorized as an automated decision. This challenge is even more apparent in today’s world where newer and more complex

¹² Commission Regulation 2016/679, art. 22, 2016 O.J., (L 119/1).

¹³ Cal. Civ. Code § 1798.185 (a)(16).

¹⁴ Automated Decision Systems Accountability Act, AB-13, 2021-2022 Regular Session (2020), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB13.



automated decision-making systems, like artificial intelligence, are used routinely in business and includes things like email spam filters and autocorrect features. Since automated decision-making is such a large part of interactions both online and offline it would be concerning for the Agency to require an opt-out option for any and every automated decision.

Instead of focusing on the overly broad category of automated decision-making technology, the Agency should consider focusing on a key subset of automated decision-making activities or uses of such technology, such as high-risk also considered “decisions with legal or similarly significant effects.”¹⁵ For example, under the VCDPA, a consumer has the right to opt-out of processing of personal data for the purposes of “profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.”¹⁶ This is further defined as “a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, healthcare services, or access to basic necessities, such as food and water.”¹⁷ Regulatory focus on high-risk use cases would align with Article 22 of the GDPR¹⁸ and specifically addressing profiling (rather than automated decision-making) would mirror other U.S. state privacy laws that IA members already comply with.

Further, regulators should only address final or fully automated decisions to ensure that their attention is properly allocated to “high-risk use cases” while not harming businesses’ ability to serve customers at scale. For example, individuals receive faster access to certain services if businesses can quickly identify low fraud risks. This is only possible at scale using either simple algorithms to approve something like a payment transaction with no prior fraud or flags or more complex algorithms that involve machine learning to identify the problem. As a result, a smaller set of fraud risk cases can then be subject to manual review for a final decision through appeals or alternative processes. If a non-final automated decision (e.g., a case being flagged by an algorithm for further human review) are regulated to the same extent as final or fully automated decisions, then consumers will be subject to slower access to services, the costs of those services will increase and there will be unnecessary manual review of commonplace, low risk practices.

B. When consumers should be able to access information about businesses’ use of automated decision-making technology and what processes consumers and businesses should follow to facilitate access.

It is important to recognize that almost every action taken online arguably involves some form of automated decision-making. Whether it is auto-completing a form, tabulating your score for a BuzzFeed quiz,

¹⁵ S.B. 1392 § 59.1-571; C.R.S. § 6-1-1303(10).

¹⁶ S.B. 1392 § 59.1-573(A)(5).

¹⁷ S.B. 1392 § 59.1-571.

¹⁸ Commission Regulation 2016/679, art. 22, 2016 O.J., (L 119/1).



redirecting a consumer from an old website to the new one, calculating a tax refund, or auto-saving an email, an automated decision is involved. It would be overly burdensome for the Agency to require businesses to provide detailed descriptions of how each process or automated decision functions. Instead, IA would ask that the Agency limit any automated decision explanations or verbiage to high-risk or “legal or similarly significant”¹⁹ occurrences as opposed to simple low risk uses and functions of automated decisions like spell check, transcription services, GPS systems and others. Any regulation of automated decision-making needs to take a risk-based approach to not only preserve a consumer’s experience, but also to provide companies with practical guidance for important high-risk automated decisions that could lead to negative profiling.

Furthermore, requiring detailed personalized explanations for all automated decisions is likely not technically feasible, it would overload consumers with information and potentially expose trade secrets, proprietary information, or violation of intellectual property rights that is essential to a business. Disclosing too much information also presents a cybersecurity risk as would-be hackers can identify vulnerabilities and exploit them, thus putting companies and their users at a significant risk. Regulations related to transparency about automated decision-making should be narrowly tailored and avoid over-inclusivity to provide reasonable processes for companies to withhold sensitive information, and balance the interest of disclosure with the risk of harm to consumers.

D. The scope of consumers’ opt-out rights with regard to automated decision-making, and what processes consumers and businesses should follow to facilitate opt-outs.

IA would strongly recommend that any regulations addressing a consumer’s right to opt-out of automated decision-making technology not deviate from the scope provided within the CPRA itself. The CPRA expressly grants consumers the right to opt-out of the sale/sharing of their personal information and for certain uses of sensitive personal information. The CPRA does not expressly grant consumers the right to opt-out of automated decision-making. Instead, the CPRA delegates rulemaking authority to the Agency to issue regulations related to the opt-out rights granted.²⁰ The statute also assigns the Agency rulemaking authority for “opt-out rights with respect to businesses’ use of automated decision-making technology,”²¹ but does not specifically create a “new” automated decision-making right to opt-out.

As such, the CPRA only allows the Agency to provide rules that allow consumers to opt-out of an automated decision-making technology when it involves a consumer’s right to opt-out of the sale/sharing of their personal information or sensitive personal information explicitly granted by

¹⁹ S.B. 1392 § 59.1-571; C.R.S. § 6-1-1303(10).

²⁰ Cal Civ. Code § 1798.185(4).

²¹ Cal Civ. Code § 1798.185(a)(16).



the CPRA. Any regulations created beyond this narrow subset or inconsistent with the CPRA itself would be considered outside of the CPPA's designated authority and thus, invalid.²²

Furthermore, there are critical exemptions to the CPRA's right to opt-out that need to be maintained in order for businesses to run frequent security checks or provide a functional product or service. However, if this Agency does decide to move forward with any limited right to opt-out right for automated decision-making when it implicates a consumer's right to opt-out of the sale/sharing of their personal information or sensitive personal information, IA would suggest that it align with the GDPR where consumers may only opt-out of solely automated decision-making by requesting human review of a decision that has caused a legal or similarly significant effects.²³

If every small or low-risk automated decision is subject to the Agency's requirements the consumer experience online will be negatively impacted. It is important that the Agency focus on high-risk automated decision-making that lead to "decisions with legal or similarly significant effects"²⁴ if they are considering regulation in this space. Additionally, there are many instances where opting-out of automated decisions would render services or products useless. For example, a map app that doesn't suggest alternative routes in response to traffic would be significantly less useful and frustrate consumers who opted out. An email inbox without a spam filter that only offered manual sorting through "human review" is another way that an unnecessary opt-out option would negatively affect consumers. There are also alternative safeguards that could be proposed by this Agency such as testing or monitoring that could be put in place as a different way to provide the consumer with the right to opt-out of certain automated decision-making processes. Ultimately, any regulations the Agency decides to move forward with around a consumer's ability to opt-out of automated decision-making features should remain consistent with opt-out rights in both Virginia's and Colorado's privacy laws.

²² See, e.g., *In re Guice*, 66 Cal. App. 5th 933, 281 (2021) (holding that the standard of review of agency regulation under Gov. Code, § 11342.2 is a two step process: first the agency's regulation must be consistent with provision that authorizes it, if it is not then the regulation is void; second, the courts evaluate if the agency is operating within its scope of authority); *In re McGhee*, 34 Cal. App. 5th 902, 908 (2019) (finding regulations adopted by the California Department of Corrections and Rehabilitation ("CDCR") void as inconsistent with the authorizing statute Prop 57, because they denied some inmates consideration by the parole board to which they were entitled under Prop 57); *Agnew v. State Bd. of Equalization*, 21 Cal. 4th 310, 333 (1999) (holding that the State Board of Equalization exceeded the scope of authority when it imposed a burden on the taxpayer which was not imposed by the statutory authority); *Henning v. Div. of Occupational Saf. & Health*, 219 Cal. App. 3d 747, 760 (Ct. App. 1990) (holding that a regulation enacted by the Division of Occupational Safety and Health that required only some asbestos contractors to register with the division was void because the statute directed that "[n]o entity shall be exempt from registration" and the regulation thus exceeded the scope of authority and was void because "[a]dministrative regulations that alter or amend the statute or enlarge or impair its scope are void").

²³ Commission Regulation 2016/679, art. 22, 2016 O.J., (L 119/1).

²⁴ Commission Regulation 2016/679, art. 22, 2016 O.J., (L 119/1); S.B. 1392 § 59.1-571; C.R.S. § 6-1-1303(10).



Topic III: Audits Performed by the Agency

IA's members would recommend that any audit authority vested in the Agency for assessing risks or issues with privacy and security have a clearly defined scope for the audit and articulated business subjects and purpose(s) for the actions being taken by the Agency. The Agency should set out formal rules of procedure for their audit process and ensure that the Agency's audit team remains separate and independent of the CPPA's investigation and enforcement teams.

Audits should not be conducted until after the Agency's regulations are finalized and should occur no more than annually for any business subject to the audit requirements. There should be at least 30 days notice provided to a company prior to an audit taking place to ensure the employees can redirect internal resources to respond and support audit requests. In addition to the notice requirement, IA would suggest that the Agency implement measures to limit the amount of data being accessed and/or collected, protect proprietary information and provide organizational measures to protect and delete the data assessed when no longer needed.

Audits reports should only be made available to the Agency upon request and the audits should not be made publicly available. The disclosure of an audit pursuant to a request from the Agency should also not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

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

Generally, IA would request a clarification in the Agency's regulations to eliminate the toll-free phone number requirement for those businesses with any physical presence as a way for consumers to exercise their privacy rights. Many IA members, especially in the sharing economy space, have small physical presences and they typically use a mobile application, a chat application, or a helpdesk email as the primary means to communicate with their customers. Moreover, the technical means of responding to consumers' requests to delete, correct, access and know their information are often not compatible with requests received via telephone. Requiring IA members such as these to continue to staff a toll-free number will be extremely burdensome on these businesses without significant benefits for consumers.

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

IA members would encourage the Agency to set out similar requirements for the "right to correct" as the Attorney General did in response to the California Consumer Privacy Act's ("CCPA") right to access and delete. Amongst these requirements the right to correct should be limited to proven factually inaccurate information and should not change things such as opinions, observations, or inferences, so as to not interfere with First Amendment principles. While evidence may not be required to change the incorrect information, in certain circumstances a consumer may be required to verify information that the consumer is requesting be changed or



such information should be made available by the consumer upon request for verification purposes. Additionally, IA members would ask, for alignment purposes, that the Agency also adopt a standard of “commercially reasonable” efforts or “reasonable steps” in order to make the changes to personal information on their services or products. This standard will allow good faith efforts to prevail when a business is identifying and attempting to make the necessary changes to the information.

Our members acknowledge that when correcting information, information pertinent to education, housing, credit, jobs or other opportunities within the U.S.’s equal opportunity framework should take priority and be addressed in a timely manner.

Topic V: Consumer’s Right to Opt-Out of the Selling or Sharing of Their Personal Information and Limiting the Use and Disclosure of Sensitive Personal Information

B. 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. (Also Includes Responses to Questions within Sections D & E)

At this time there is uncertainty about a global opt-out option or signal because there are no principles proposed for its creation, implementation, ubiquity, and limitations where appropriate. Furthermore, the CPRA’s language makes a global opt-out an optional feature that is not required. Therefore, if this Agency decides to move forward with some type of global opt-out rules it should recognize IA’s concerns and recommendations about the reality of a global opt-out signal.

First, if a centralized opt-out is created through private actors at the browser or operating system level it may create incentives for companies to design and manage these controls in a way that harms competition. Thus, we would recommend that any device/signal not be left to a single company or organization to create and oversee, but instead developed and tested by the internet ecosystem itself. A global opt-out signal should be flexible, technology neutral, and be a collaboration of industry efforts, so that there is some type of consensus as to the signal’s standards and a variety of businesses are able to comply.

Second, we would suggest that the Agency consider guidance for companies about how to handle competing signals when a person opts-out through a global control, but then opts-in to receive a specific service. Without this guidance businesses will experience the creation of multiple signal types and varying standards for their use, which will ultimately increase compliance costs and have a negative impact of honoring consumers’ choices about the collection and use of their personal information. Finally, there should be a method within this global opt-out system to allow businesses to maintain their relationships with consumers without conforming to another



business' standard. There should also be a way for businesses to win back their consumers after they make and rectify mistakes when it comes to handling personal information. Without considering some of these challenges a global opt-out signal will be difficult to implement and will not produce the intended benefits for consumers.

IA members would also recommend that the Agency provide more clarity and examples for the term "sharing in a cross-contextual behavioral advertising context" as related to the global opt-out. The text of the CPRA itself does not seem to address this issue. Further, when issuing guidance around this terminology the Agency should be as precise as possible to ensure compliance.

Topic VI: Limiting the Use and Disclosure of Sensitive Personal Information

As a starting point IA members believe that the Agency should take this rulemaking opportunity to consider aligning the future actions surrounding CPRA's definition of sensitive personal information with that of VCDPA²⁵ and CPA²⁶ to more accurately reflect a consumer's sensitive information such as race or sexual orientation and eliminate less sensitive personal information such as philosophical beliefs. This alignment will provide businesses with clearer direction when they are trying to comply with multiple privacy laws across state lines.

IA would also encourage that any changes to limiting the use and disclosure of sensitive personal information not include information that has been de-identified or whose disclosure was reasonably necessary to provide the service requested by the consumer. Many of our members are taking steps to further protect consumers' sensitive information, and excluding de-identified information under this requirement would continue to incentivize that behavior. We would also ask that the appropriate carve outs, like those in the exceptions section of the CPRA²⁷ be preserved to continue to allow our members to proactively work with law enforcement, keep accurate employment records,²⁸ and enhance security measures of this information to further protect it.

Topic VIII: Definitions and Categories

As previously stated above, IA members are extremely supportive of consistent privacy standards across state lines, as this provides dependable expectations for consumers exercising their rights and provides clear guidance for businesses implementing privacy laws at a rapid rate. We suggest

²⁵ See S.B. 1392 § 59.1-571 (defining sensitive data).

²⁶ See C.R.S. § 6-1-1303(24).

²⁷ See Cal. Civil Code § 1798.145.

²⁸ If there are any regulations in the HR context, they must: (1) not impose undue burden; (2) permit an opt-out process through existing internal HR platforms and technologies; and (3) not conflict with the ability to comply with state and federal laws; civil, criminal, or regulatory inquiries, investigations, subpoenas, or summons; or to exercise or defend against legal claims.



that the Agency keep harmonization top of mind when considering our definition and categories recommendations.

B. Updates or additions, if any, that should be made to the categories of “sensitive personal information” given in the law.

Please see “Topic 6” above for our recommendations about the sensitive personal information definition.

C. Updates, if any, to the law’s definitions of “de-identified” and/or “unique identifier.”

IA members support aligning the definition of “de-identified information” with that of Virginia.²⁹ This would require that the Agency update the definition to provide further separation between “pseudonymized” and “de-identified” personal information by applying exceptions to “pseudonymized” information similar to that in the VCDPA; remove the reference to “inferring information”; and add a reference to devices linked to a consumer.

We would also suggest removing references to devices “linked to the consumer” as examples of unique identifiers. As we noted in our comments to the Attorney General’s office during the CCPA rulemaking process³⁰ devices can be shared by multiple consumers in the household. It’s common for multiple members of a household to share tablets or other devices. Thus, we recommend alignment with the VCDPA on this point.

G. The changes, if any, that should be made to further define “precise geolocation.”

We would encourage the Agency to further synonymize the CPRA’s definitions with that of Virginia³¹, particularly when it comes to precise geolocation. Specifically, we would request that “precise geolocation information” not include de-identified information or the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

J. The regulations, if any, that should be adopted to further define “dark patterns.”

The CPRA’s definition of dark patterns is overly inclusive and would be extremely difficult for companies to implement. Rather than describing the elements of dark patterns, the definition focuses on limiting consumers’ autonomy, decision-making, or consumer choice. To some extent all services or products have an impact on consumers because they are presented with content and options in different ways to enhance the consumer’s ability to interact with the service or

²⁹ See S.B. 1392 § 59.1-571 (defining deidentified data as data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person).

³⁰ Internet Association Comments on California Consumer Privacy Act of 2018 Initial Rulemaking, California Attorney General’s Office, <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf> (last visited November 8, 2021).

³¹ See S.B. 1392 § 59.1-571 (defining precise geolocation).



product. Therefore, the definition of dark patterns as drafted is difficult, if not impossible to comply with.

Additionally, because this is a new area of regulation, IA members would note that any regulations the Agency introduces will need to provide significant and specific guidance. IA members would strongly encourage the Agency to provide examples of dark patterns and the behaviors that they are looking to deter and consult with web and application designers to understand the constraints of the requirements the Agency puts forth. However, the Agency should also be careful to provide an overly prescriptive approach to these regulations due to the varying business models subject to the law and the impact these regulations have on the user experience and expectations of the products they use. To a certain extent all interfaces impair autonomy and choice, specifically, under the current definition of “dark patterns” in the CPRA, some IA members are concerned that they may be limited in their ability to provide privacy protective settings due to the broad language. As an unintended consequence, overly prescriptive regulations could cause a consumer to turn on location sharing where they have previously turned off that setting to share their location information. IA members would like to be active stakeholders in this process and we hope to work with the Agency on this emerging area of regulation.

Topic IX: Additional Comments or Considerations

A. Disclosing trade secrets.

While the CPRA statute indicates that nothing within the text that “shall require a business to disclose a trade secret”, IA members would also recommend that the Agency reiterate this principle throughout the rulemaking process, especially when it comes to ADS. California’s own Uniform Trade Secrets Act and the federal Defend Trade Secrets Act recognize the importance of trade secrets that have been developed through a combination of time, resources, expertise, and talent. Trade secrets are critical to protecting businesses’ intellectual property and an explicit exception in the Agency’s rulemaking process would allow companies to continue to innovate and continue to grow the U.S. economy.

B. Clearly labeled link to privacy choices on a business’s internet homepage.

We would also ask that the Agency provide further clarification about what specifically constitutes a “single, clearly labelled link on the business’ internet homepage.”³² We suggest that there be flexibility for this requirement given different business products, services, and models. If the link is clearly labeled (e.g. Privacy Controls, Privacy Preferences, Privacy Choices) and takes the consumer to a tool or other mechanism that allows the consumer to immediately access their

³² Cal. Civ. Code § 1798.135(a)(3).



choices when it comes to limiting use of sensitive personal information or opting-out of the sale/sharing of personal information, it should be seen as compliant.

Conclusion

IA members know that these practical questions are urgent matters in need of clarification as businesses design compliance systems, processes and train personnel in anticipation of the CPRA statute and regulations becoming effective in 2023. We ask that the Agency act swiftly with clear and specific guidance to provide businesses as much time as possible to adapt their systems to these additional requirements. To assist in this process IA members would again encourage consistency in privacy requirements across state lines where appropriate to allow for businesses to come into compliance with all three privacy laws and subsequent regulations as quickly as possible.

We look forward to continued engagement and cooperation in the future rulemaking process and if you have any questions please feel free to reach out to Dylan Hoffman, Internet Association's Director of California Government Affairs at [REDACTED].

Respectfully,

A black rectangular box redacting the signature of Dylan Hoffman.

Dylan Hoffman
Director of California Government Affairs
Internet Association

A black rectangular box redacting the signature of Alex McLeod.

Alex McLeod
Legal and Policy Counsel
Internet Association

From: Jennifer King PhD [REDACTED]
Sent: 11/8/2021 8:18:31 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Eli McKay MacKinnon [REDACTED]; James Yang Zou [REDACTED]; Divya Nagaraj [REDACTED]; Mitch M Bennett [REDACTED]
Subject: PRO 01-21 Comments
Attachments: Stanford_CPRA_Comments_final.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

.....
Please accept these comments in response to the CPRA's PRO 01-21 proposed rulemaking on behalf of Jennifer King, James Zou, Eli MacKinnon, Mitch Bennett, and Divya Nagaraj of Stanford University.

Sincerely,

Jen King

Jennifer King, Ph.D (she/her)
Privacy and Data Policy Fellow
Stanford Institute for Human-Centered Artificial Intelligence
hai.stanford.edu

https://urldefense.proofpoint.com/v2/url?u=https-3A__hai.stanford.edu_people_jennifer-2Dking&d=DwIGaQ&c=LHIwbLRMLqgNuqr1uGLfTA&r=V4xunG0ycYpaxqwPk-6b0S7HvhVBD1m5-sXl-MDFdxk&m=-A7ZFyKIER7Iaa-6bCA05zYmiocxxgpoBwo8XQuYJ2uC4nfqkjwqxVoXBB1lzzTk&s=wBwm52bXbPNjibMb4I4vGDKd3p7n6whJyyht3bfHqc&e=https://urldefense.proofpoint.com/v2/url?u=http-3A__www.jenking.net_publications&d=DwIGaQ&c=LHIwbLRMLqgNuqr1uGLfTA&r=V4xunG0ycYpaxqwPk-6b0S7HvhVBD1m5-sXl-MDFdxk&m=-A7ZFyKIER7Iaa-6bCA05zYmiocxxgpoBwo8XQuYJ2uC4nfqkjwqxVoXBB1lzzTk&s=5Hpwx9ly-o5XwzxBwgAuah4Tns4MmQJte3pZCGsnvsw&e=Google Scholar profile: https://urldefense.proofpoint.com/v2/url?u=https-3A__scholar.google.com_citations-3Fuser-3D05jENBMAAAJ-26hl-3Den&d=DwIGaQ&c=LHIwbLRMLqgNuqr1uGLfTA&r=V4xunG0ycYpaxqwPk-6b0S7HvhVBD1m5-sXl-MDFdxk&m=-A7ZFyKIER7Iaa-6bCA05zYmiocxxgpoBwo8XQuYJ2uC4nfqkjwqxVoXBB1lzzTk&s=tBi2eH_1wBT_Ajeh8KHSZsYg14aQYutFPNWAQbn8Bwo&e=



Stanford University
Human-Centered
Artificial Intelligence

November 7, 2021

California Privacy Protection Agency
915 Capitol Mall Ste. 350A
Sacramento, CA 95814

Via email: regulations@cppa.ca.gov
Re: PRO 01-21

We are pleased to submit comments in response to the California Privacy Protection Agency's Sept. 22 invitation (Proceeding No. 21-01) for proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA). We are a group of academic researchers and students affiliated with Stanford University and the Stanford Institute for Human-Centered Artificial Intelligence (HAI), and we provide our affiliation for informational purposes only; our comments are made on behalf of ourselves and do not represent the views of either Stanford University or Stanford HAI.

The Agency asked for comment on specific aspects of the CPRA, and we include here several responses as well as additional comments based on our research over the past year on aspects of the CPPA. Our group offers our comments based on our academic expertise and professional experience in the fields of information science (human-computer interaction), computer science (artificial intelligence), and technology policy. The comments are included in the following document.

Thank you for the opportunity to submit comments on these timely and important topics of relevance to all Californians.

Sincerely,

Jennifer King, Ph.D
Data and Privacy Policy Fellow, Stanford Institute for Human-Centered Artificial Intelligence

James Zou, Ph.D
Assistant Professor of Biomedical Data Science and, by courtesy, of Computer Science and of Electrical Engineering, Stanford University

Eli MacKinnon
Graduate Student Researcher, Stanford University

Mitch Bennett
Graduate Student Researcher, Stanford Law School

Catherine Baron
Undergraduate Student Researcher, Stanford University

Divya Nagaraj
Undergraduate Student Researcher, Stanford University

Summary of Recommendations

Topic Two: Automated Decisionmaking

1. We recommend the Agency narrow the scope of covered automated decisionmaking technologies (ADT) to those that relate to a specific outcome of concern, whether it be similar to the GDPR's focus on legal effects, or another interpretation that focuses more directly on outcomes related to consumer privacy.
2. "Profiling" notices should be delivered at a point when consumers can make an actionable decision on whether to submit, and businesses must be incentivized or required to offer substantive alternatives that don't involve the use of profiling.
3. Regarding the provision to consumers of "meaningful information about the logic" of automated decisionmaking processes, we suggest that transparency regarding the data being used to power such processes may be of greater consequence. Giving consumers actionable instructions on how they can prevent such data from being incorporated into automated decisionmaking processes is preferable to focusing exclusively on these processes' logic, which is often hard to interpret even for their designers.
4. Data embedded within machine-learning models must be explicitly covered with respect to consumers' rights to delete, know and correct. This will require regular retrainings of models and potentially the use of novel techniques such as "approximate deletion."

Topic Four: Consumers' Right to Delete, Right to Correct, and Right to Know

5. Businesses should be required to document the source of sensitive personal information they possess on a given consumer, including current contact information for the source parties and whether the information was obtained with explicit and documented consent.
6. In cases where sensitive personal information is not actively needed for exempted business operations and the consumer has not explicitly consented to the collection and use of this information for some other purpose, businesses should be required to permanently delete sensitive personal information by default within a specified time period, even without being requested to do so.

Topic Five: 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

7. CPRA regulations should provide unambiguous language clarifying that global privacy signals, such as the Global Privacy Control (GPC), do not represent merely one among several possible opt-out signals that businesses can choose to recognize, but are instead obligatory to recognize for all businesses.
8. Any browser downloaded by a California consumer, as defined in §1798.40(i), should come with built-in support for GPC and have GPC set on by default.
9. Given potential loopholes, the Agency should require that support for global privacy signals such as GPC be offered in addition to conspicuous opt-out links, not as a replacement sufficient to negate that requirement.
10. Opt-out preferences expressed via one medium (such as a website) should apply automatically to any others (such as an associated mobile app), if it is known from previously collected data that a consumer has expressed such a preference via another medium.
11. Privacy within the mobile app ecosystem, which currently offers no equivalent to the Global Privacy Control, must be prioritized alongside in-browser privacy. The Agency should mandate that apps approach the exercise of CPRA rights in a way that's already been demonstrated to work: a pop-up dialogue displayed upon first use of an app.

Topic Six: Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information

12. We recommend that the Agency consider 'precise geolocation' data as a suitable candidate for inclusion in further statutory exemptions from the right of an individual to limit the use and disclosure of SPI; we suggest that precise geolocation data could be collected and processed within a narrow and pre-specified context of use, subject to the limitations we address inline. Further, we recommend that the Agency consider requiring the deletion of this data after delivery of a product or service.

Topic Eight: Definitions and Categories

- 13.** Given the increasing use of AI to attempt to detect or measure individuals' "emotions" and "emotional states," we recommend that these terms comprise their own category of personal information (and potentially, sensitive personal information).
- 14.** The Agency should consider amending the definition of 'sensitive personal information' (SPI) to include inferences that can be characterized as SPI drawn from non-SPI personal information.
- 15.** The Agency should consider amending the definition of "deidentified" to provide further clarity in respect to the reasonableness standard applied to the reidentification risk of anonymized information.
- 16.** We suggest revisions to either the definition of "dark patterns," or to related terms incorporated by reference, in order to allow for a broader interpretation of what constitutes a dark pattern that encompasses novel interfaces, such as voice, that go beyond traditional visual user interfaces.

Topic Nine: Additional Comments

- 17.** Annual Reporting Requirements: CCPA reporting requirements currently produce results that are difficult to collect, compare, and evaluate compliance. We offer several recommendations to improve annual reporting requirements, based on ongoing research by co-author Catherine Baron.
- 18.** Dark Patterns: We provide recommendations to the Agency, via co-author King's recently published work, as to how to further regulation and oversight on this topic beyond consent interfaces.

Topic Two: Automated Decisionmaking

Regarding the use of “profiling” and “automated decisionmaking technology” (ADT), the text of Proposition 24 reads that the Agency will: “Issu[e] regulations governing access and opt-out rights with respect to businesses’ use of automated decisionmaking technology, including profiling and requiring businesses’ response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.” Further, “profiling” is defined in the text of Proposition 24 as meaning: “any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.” This definition appears to have been modified from Recital 71 of the General Data Protection Regulation (GDPR).¹

We are concerned that the current language of Proposition 24 invites an interpretation that will have the unintended consequence of targeting many algorithmic processes that do not pose inherent privacy risks to consumers. In particular, a key aspect of Recital 71 was omitted from the proposition text: “The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.” Recital 71 incorporates the GDPR’s definition of automated processing given in Recital 22, which narrows the applicability of automated processing to decisions which produce *legal effects*.² No corresponding definition of automated decisionmaking is included in the proposition text, without which, the applicability of ADT can be broadly interpreted to include any form of ADT whether it presents a privacy risk, or a ‘legal effect,’ or not.

We recommend the Agency revise this section to narrow the scope of ADT as it relates to a specific outcome of concern, whether it be similar to the GDPR’s focus on legal effects, or another interpretation that focuses more directly on outcomes related to consumer privacy. We also recommend that the Agency refine the definition of profiling to focus on the range of processes, automated or not, that contribute to the specific outcomes of concern: the generation of inferences, predictions, and evaluations about individual

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679> (Recital 71).

² Ibid (Recital 22).

consumers or groups of consumers conducted without their control, knowledge, or consent. To that end, it bears mentioning that the activity of profiling itself is only one component of this issue; the business practices and technological processes that enable profiling should also be addressed.

We are concerned that an overbroad application of this provision could force the unnecessary labelling of an immensely broad number of ADTs with no privacy risk, providing no useful outcome for California consumers. To the extent that this regulation deliberately or inadvertently targets specific ADTs such as those built using artificial intelligence (AI), and more specifically, machine learning, addressing specific concerns would be better served in separate regulation, where issues related to the data that feeds AI systems can be addressed directly.

We address the specific points that the Agency has asked for guidance on in turn below:

(a) *What activities should be deemed to constitute "automated decisionmaking technology" and/or "profiling"?*

As described above, we are concerned with both the current definitions of ADT and profiling in §1798.185 (16)(a) and this request for comment. At the present level of generality, any algorithmically driven process could be encompassed by this provision, which could have far-reaching negative effects on consumers' online experiences. There are many ADT processes online that have no direct impact on consumer privacy. For example, car rental agencies use ADTs to ask for a consumer's age before displaying rental opportunities. Retail stores may ask for an address or zip code in order to present a list of nearby store locations. In these instances, if the data is used only for the provisioning of the immediate product feature, deeming these types of ADTs as requiring notice through labeling, as well as requiring an explanation of their logic, offers no clear consumer benefit, nor an inherent privacy risk.

It is important to distinguish profiling as a practice of concern distinct from ADT generally. The use of the term "profiling" implies data collection practices, either by a first-party data collector or by one or more third parties, that result in the aggregation of data about an individual³ that can then be used to classify the individual, group them with other individuals on the basis of one or more characteristics, or make predictions or inferences about them based on past behaviors, actions, preferences, or traits held in common with others. Profiles can be deliberately constructed through the analysis of aggregated data, or emergent, based on identifying correlations between variables without a specific

³ The data collected through aggregation can be exceedingly diverse, and in addition to specific facts such as demographic data can include mechanisms such as behavioral tracking using browser cookies or third party pixel tracking via web pages, browser fingerprinting, location data, IP addresses, and other similar forms of tracking deployed through mobile apps (both via the apps and third party code embedded within them).

hypothesis (i.e., “data mining”). Profiles can be built through human analysis or through the application of artificial intelligence (e.g., machine learning), and once constructed applied through both manual (human in the loop processes) as well as ADT-based mechanisms. We are concerned that the current definitions of ADT and profiling could exclude profiling practices that do not rely on ADT, or incentivize companies to skirt the regulation by nominally including a human decisionmaker in the process, even if their contribution is minimal.

Given that not all forms of profiling may result in the uncontrolled or adverse collection of personal information, the Agency should consider which practices pose substantial privacy risks, both to individuals as well as groups, or even to society at large. The Agency should also identify the specific practices that enable first and third-party companies to collect and aggregate the data that enable building consumer profiles, in particular those practices that occur without explicit consumer knowledge and consent. For example, some low-level forms of first party website personalization, such as saving a user’s preferences, may pose a low privacy risk to consumers as long as the data is collected and used only for this specific purpose and not later sold, shared, or reused outside this context.

Profiling practices that utilize machine learning (ML) bear particular mention here. As we elaborate in further sections below, there are assumptions embedded in the articulations of profiling in the proposition text that are based on conventional non-ML processes, and which may not apply directly to ML-based profiling. ML models are built upon training data—data selected and labeled as representations of specific types of actions or characteristics—that ML algorithms utilize to “learn” and, in the case of consumer profiling, use the results to analyze data and create emergent classification schemes. Instead of a human data scientist analyzing statistical models to identify correlations and create profiles, ML algorithms can create profiles based on the predictions of the trained ML model. This process implicates a different set of challenges for responding to issues of deletion and opting out of them, as we discuss below.

(b) When consumers should be able to access information about businesses’ use of automated decisionmaking technology and what processes consumers and businesses should follow to facilitate access.

The timing of any profiling notices should occur at a point where consumers can make an actionable decision on whether to submit, or not, to a profiling-based process, while keeping in mind the many empirical research findings that have demonstrated the challenges with providing effective and meaningful notice.⁴ While providing notice may

⁴ There is substantial academic literature on this topic, but to offer two overview citations: Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space For Effective Privacy Notices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15)*. USENIX Association, USA, 1–17; [Privacy](#)

imply that consumers have a meaningful *choice* to decline to participate, it does not guarantee that they have a meaningful *alternative*. If providing notice, or labeling, of profiling is intended to follow in the model of notice and consent, then the practice is, unfortunately, futile. Forcing companies to provide notice of profiling if there is no substantive action consumers can take may be confusing at best, frustrating at the very least, and fail to curb use of profiling through public exposure of the practice.

Furthermore, providing notice, or labeling, of profiling may be especially complex given that the creation of profiles themselves likely does not happen in real time when a consumer uses a product. Unless instructed otherwise, companies will bury any notice regarding profiling technologies into their privacy policies, documents that it is well established consumers do not read. As presently written, companies would be incentivized to simply give a notification using the same “take it or leave it” terms that currently exist throughout the online sphere without altering their existing practices, which some have rightly called “consent theatre.” If the goal is to curb the excessive or exploitative use of ADTs that undermine privacy, businesses must be incentivized or required to offer substantively the same service without the use of profiling.

(c) What 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.

It is unclear that providing consumers with meaningful information about the “logic” behind an automated profiling process will be beneficial unless, again, consumers have substantive options to avoid it.

There have been research-driven attempts to provide people with increased transparency around AI and automated decision models.⁵ The results are unclear and have raised concerns about the effectiveness of directly passing information, such as model parameters and weights, to users. Even if such information would prove useful to an algorithmically literate individual, it is unclear whether it would substantially impact their actions on a platform. A second large challenge related to algorithmic explainability is that even machine learning engineers, the architects of the very algorithms being analyzed, often cannot interpret the contributions of various weights to the final prediction of the algorithm. Current research aims to improve the interpretability of key models in specific

[and Human Behavior in the Age of Information](#), Acquisti, Alessandro and Brandimarte, Laura and Loewenstein, George. *Science*, 347 (6221), 509–514, 2015.

⁵ For example, see: Linardatos, P.; Papastefanopoulos, V.; Kotsiantis, S. Explainable AI: A Review of Machine Learning Interpretability Methods. *Entropy* 2021, 23, 18. <https://dx.doi.org/10.3390/e23010018>; Katherine Miller. Should AI Models be Explainable? That Depends. March 16, 2021, available at: <https://hai.stanford.edu/news/should-ai-models-be-explainable-depends>.

domains—like facial recognition—but at present, there are no guarantees that any gains in interpretability resulting from this research will generalize to other models and systems.

Given these significant challenges around algorithmic interpretation, we suggest that what may be of greater consequence is transparency regarding the *data being used to power such processes*, with clear instructions to consumers as to how they can prevent such data from being incorporated into profiling processes, rather than focusing exclusively on the logic of the process itself.

We ask the Agency to consider requiring companies to document the source of all the data they collect, purchase, or trade, including documentation regarding whether or how the consumer was asked to consent to the collection of the data. We conjecture that if companies had to document the provenance of the data they collect, and present this information to regulators and to consumers, then consumers might be able to draw meaningful conclusions from companies' use of it. For example, if information brokers had to reveal all sources of all data collected about an individual (including the contact information for the source parties), a consumer armed with such detail might be able to trace the origins of particular data points, including incorrect or outdated information. To an extent, credit reporting bureaus are required to engage in a form of this practice today. Within the context of privacy, this may be a more powerful and relevant approach than requiring transparency of ADT logic alone.

(d) The scope of consumers' opt-out rights with regard to automated decisionmaking, and what processes consumers and businesses should follow to facilitate opt outs.

If labeling profiling is to be effective, then consumers need to be given actionable options to refuse it, as well as reasonable and realistic alternatives to the profiling-based service. The take-it-or-leave-it terms that consumers are offered today force many to engage with companies or with business practices that they would otherwise prefer not to, given that in many cases they lack other options. However, the Agency's determination of what constitutes legitimate profiling will matter here, as presumably there are some products or services for which it would be difficult to offer a viable alternative. We offer more specifics regarding the challenges and consequences of opting out of ADTs based on artificial intelligence in our comments on Topic 4 below.

Topic Four: Consumers' Right to Delete, Right to Correct, and Right to Know

Regarding consumers' rights to correct, delete and know what personal data a business has collected, we alert the Agency to the need to plan for the subtleties that such rights will

entail when applied to personal data used to train machine learning (ML) models. While it is easy to imagine some piece of personal information as an inert entity in a data table — easily deleted or corrected — the reality is that a business can quickly propagate information through the tools it uses in ways that create obstacles to straightforward removal and alteration. In particular, data used to train ML models becomes “embedded” in those models in ways that are not easily reversed. In spite of the relative difficulty posed by amending the data that undergirds actively deployed ML models, privacy rights must extend to this data in order to be meaningful; in exactly these contexts, data carries far-reaching impacts and the potential for unwanted distribution and disclosure.

ML models are first trained on one dataset before being applied to the analysis of novel data. For example, an employment screening business might collect information on a broad range of individual characteristics, such as age, geolocation, educational background and past purchasing behavior, before using this data to train a filtering algorithm for job applicants. In the training phase, the algorithm will surface correlations between individuals’ specific personal characteristics and their success as job applicants with respect to some role. Then, when the training is complete, this algorithm will be used to infer the suitability of new applicants—classifying them based on how well they match the patterns embedded in the training data. Imagine that a California consumer whose data was used to train the model requests this business delete their data. At this stage, even if their individual record were deleted, their contribution to the ML model would remain intact until the model is retrained on an updated data set.

As long as the model remains in use, any erroneous, outdated or simply unwanted correlations that an individual’s data contributed to will continue to manifest and subvert the relevant individual’s rights over their personal information. In fact, failure to remove data from ML models would directly nullify a consumer’s ability to meaningfully control the use and potential spread of their personal information: Researchers have shown that under some conditions, original training data can be reconstructed and ultimately deanonymized by analyzing the behavior of an ML model that incorporates it.⁶ While an individual’s data remains embedded in a model, it cannot be said to have been deleted. The Federal Trade Commission supported this view in a recent settlement with a photo-sharing app that allegedly deceived consumers about how it was applying facial-recognition technology — the settlement required that all models and algorithms trained using the data be deleted along with the original photo data.⁷

⁶ Salem, et. al. *ML-Leaks: Model and Data Independent Membership Inference Attacks and Defenses on Machine Learning Models* (February 2019).

⁷ *Everalbum, Inc., In the Matter*. Case summary and decision available at: <https://www.ftc.gov/enforcement/cases-proceedings/192-3172/everalbum-inc-matter>.

If a consumer requests deletion or alteration of their data used in an ML model, the most straightforward way for a business to honor the request is to retrain every ML model in which these data were included. Retraining an ML model is not a trivial process and can be both time-consuming and expensive, given the computational resources required to analyze vast datasets. For this reason, we anticipate that the Agency will see significant pushback from businesses wishing to avoid such a responsibility and potential cost center. This pushback may include arguments proposing, in effect, that deleting or altering data already embedded within an ML model is onerous or virtually impossible.

The Agency should reject such arguments and ensure that data embedded within ML models are explicitly covered with respect to consumers' rights to delete, know and correct. While retraining models is time- and resource-intensive, businesses of the size and specialization covered by the CPRA already routinely retrain models to improve them as new data are collected. Additional retrainings for the purposes of honoring CPRA requests are both feasible and necessary to honor the law's intent, and any subsequent regulation should be written with this requirement in mind, particularly with regards to timing requirements. Moreover, the understanding that data included in ML models is subject to deletion and alteration requests will incentivize businesses to be both more conservative in their collection and use of personal data, and more explicit in communicating to consumers which data they use and how they use it, as well as in obtaining consent—businesses will be motivated to avoid mandatory retraining or penalties resulting from the misuse of individuals' personal information.

In addition to retraining ML models on new data, there are other avenues for promptly honoring consumer data rights. A team of researchers from UC San Diego and Stanford University, including Professor James Zou, a co-author of this comment, has advanced a technique called "approximate data deletion."⁸ Using this technique, the impact of specified data on an ML model can be quickly and cheaply negated, so that the potential for deducing these data in their raw form is greatly reduced or eliminated. The application of this method or a similar one would also allow businesses to respond to user requests immediately and without taking a model offline during retraining — it therefore might form a stopgap that could be used by businesses to honor consumer data rights before they've had an opportunity to fully retrain a model with relevant data deleted.

⁸ Izzo, Smart, Chaudhuri and Zou, *Approximate Data Deletion from Machine Learning Models* (April 2021). Available at: <http://proceedings.mlr.press/v130/izzo21a/izzo21a.pdf>.

Topic Five: 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 rules and procedures should be established to allow consumers to limit businesses' use of their sensitive personal information.*

As previously discussed in regard to Topic Two above, we believe consumers' control of their personal information must be rooted in transparency around the information's provenance—this is especially true in the case of sensitive personal information. Businesses should be required to document the source of sensitive personal information they possess on a given consumer, including current contact information for the source parties and whether the information was obtained with explicit and documented consent. Businesses should supply this information to consumers, at minimum in their data privacy disclosures. While not a substitute for an outright ban on non-consensual collection, such disclosures could help empower consumers not only to limit a first-party business's use and disclosure of their sensitive personal information to those exempted purposes explicitly outlined in CPRA, but also to identify specific third-party sources, and, if they wish, take steps to limit its continued spread from those sources as well. A measure such as this would help close one of the existing loopholes in the CCPA: that even with "do not sell" and deletion rights, consumers often have no idea to whom to make these requests beyond the businesses with whom they have first-party relationships.

We also advise that, in cases where sensitive personal information is not actively needed for exempted business operations and the consumer has not explicitly consented to the collection and use of this information for some other purpose, businesses should be required to permanently delete sensitive personal information by default within a specified time period, even without being requested to do so. Barring such a provision, we expect that the CPRA's broad language exempting the collection and use of sensitive personal data for specific purposes (e.g. ensuring "security and integrity") will be abused by businesses to hoard sensitive personal information without meaningful justification.

- b. 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.*

As the Agency is clearly aware, based on the important addition to the CPRA of new language prohibiting the use of dark patterns in certain contexts (see “Topic Eight: Definitions and Categories” below for additional discussion), there is a pressing need to standardize the processes by which consumers express their preferences regarding the sale and sharing of their personal information, as well as the use and disclosure of their sensitive personal information. Presently, opt-out preferences are inconsistently designed, can be hard to find, and provide opportunity for consumer manipulation. Best Buy customers, for example, if they manage to locate the “Do Not Sell My Personal Information” link in small print at the bottom of the electronics retailer’s homepage, will be greeted with a lecture on the technical definition of the word “sale” before seeing instructions on how to opt out.⁹ Though this explanatory text makes mention of a “Do Not Sell My Personal Information” button, a mention which itself could easily be made an interactive link, the button is located further down the page and relegated to the left margin.

Such unnecessary friction is typical, but there is a deeper problem. Even after a consumer completes an opt-out process, that opt-out signal is only valid on a specific device and on a specific browser whose cookies have remained unaltered since the point in time when the opt-out signal was registered. Privacy-minded consumers are perhaps especially likely to regularly delete their browser cookies, negating past opt-out requests in the process, and businesses are therefore incentivized to wage a war of attrition on consumer data preferences. While appearing to honor consumer preferences around their personal information, businesses need only wait for consumers to switch to a new device, a new platform, such as an app, or a new (or just newly reset) browser — perhaps at a time when they are in too much of a hurry to initiate a new opt-out process — before they can safely resume data sales and sharing.

This is why an automatic opt-out mechanism like the Global Privacy Control (GPC) is crucial for supporting consumer privacy in our present data ecosystem—it allows consumers to efficiently and persistently communicate opt-out signals, and to defend against businesses that would try to exploit the ephemerality of manual opt-out requests to subvert their privacy preferences. The CPRA includes language in §1798.135(b)(1) describing opt-out signals sent via “a platform, technology, or mechanism,” such as the GPC, and as former Attorney General Becerra clarified last summer, “under law, [GPC] must be honored by covered businesses as a valid consumer request to stop the sale of personal information.”¹⁰ However, CPRA regulations should go further and provide unambiguous language clarifying that the GPC is not merely one among several possible opt-out preferences that businesses can choose to recognize, but an opt-out signal that is

⁹ BestBuy.com. Accessed Nov. 2021 via: <https://www.bestbuy.com/site/california-privacy-rights/do-not-sell/pcmcat1576178819013.c?id=pcmcat1576178819013>

¹⁰ “CCPA Frequently Asked Questions.” State of California Department of Justice. Accessed Nov. 2021 via: <https://oag.ca.gov/privacy/ccpa>

obligatory to recognize for any business that is technically capable of doing so (in effect, any business, excluding those that fall under the requirements of the CPRA despite not having a website). Such an addition would help resolve the apparent inconsistency between §1798.135(b)(1) and §1798.135(e), the former of which seems to position global preference signals like GPC as one CPRA-compliant option and the latter of which says that businesses must honor global opt-out signals in all cases. Universal recognition of the GPC will ensure that it empowers consumers to exercise their data preferences in a sustainable manner within a current landscape of inconsistent, often inconspicuous and (thanks to frequent changes in consumers' browser cookies and preferred devices) ephemeral opt-out request processes.

It's important, though, that GPC is not only universally recognized but also universally available. Though GPC is gaining traction, it's currently not supported by either of the U.S.' two most popular browsers—Chrome and Safari, which together account for 84.62% of installed browsers in the U.S.¹¹ In fact, only one of the country's nine most popular browsers supports it—Firefox, whose share of U.S. browsers is just 3.53%. Given GPC's crucial utility in realizing CPRA's aims, as well as its extreme simplicity and ease of implementation, we recommend that the Agency require any browser downloaded by a California consumer, as defined in §1798.40(i), come with built-in support for GPC and have GPC set on by default.

The GPC's current lack of wide availability creates other threats to CPRA's ultimate effectiveness. As discussed above, the CPRA could currently be interpreted to position the GPC and other similar tools as *alternatives* to the standard opt-out process defined by the CCPA—namely, a conspicuously placed link or set of links on a business's homepage. Section 1798.135(b)(1) reads, in part: "A business shall not be required to comply with subdivision (a) if the business allows 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, based on technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185..." The aforementioned subdivision (a), with which a GPC-recognizing business is not required to comply, specifies the need for a link or pair of links that consumers can use to express a preference signal with respect to personal information and sensitive personal information.

For a consumer who was not using a GPC-enabled browser or another equivalent mechanism when interacting with a business that had opted to support GPC and exempt itself from the requirements of Section 1798.135(a), there would not necessarily be any other clear method by which to express an opt-out signal. Given that, as detailed above,

¹¹ "Browser Market Share United States of America." StatCounter Global Stats. Accessed Nov. 2021 via: <https://gs.statcounter.com/browser-market-share/all/united-states-of-america>

the most popular browsers don't currently support GPC, companies might choose to support GPC as a means to avoid offering a more broadly accessible opt-out signal, such as a conspicuous link. We therefore recommend the Agency require that GPC be supported *in addition* to conspicuous links, not as a replacement sufficient to negate that requirement, in order to close any potential loopholes for consumers.¹²

Consumers currently face another obstacle in expressing their opt-out preferences. Revisiting Best Buy's "Do not sell my information" page, we see the retailer's concise statement of this issue: "Your selection won't cross from the website to mobile application (or the other way round): If you click the "Do Not Sell My Personal Information" on this website, your selection will not transfer to our mobile app. Similarly, your activation of the feature on the mobile app won't apply to bestbuy.com. You'll need to do both."¹³

There are cases in which such siloing of preferences between browsers and apps is unavoidable. For one, it's possible that a business whose website is visited by a consumer who also uses its mobile app has simply not identified them as the same person. However, it's very common that businesses *do* positively match the identity of a website visitor with an app user, via a login, a unique device ID or some other fingerprinting mechanism, though these comments should not be read to promote the use of such practices for the purposes of profiling. In such cases, there is no technical reason why a request submitted via one medium could not be automatically applied to the other, and in terms of consumer preferences, there is no reason why it should not be. After all, behind the distinct access points, it is the same business with the same data, the same data practices and the same incentives. We therefore recommend that the Agency require opt-out preferences expressed via one medium (such as a website) to apply automatically to any others (such as an associated mobile app), if it is known from previously collected data that a consumer has expressed such a preference via another medium.

Mobile apps present other important challenges with regard to opt-out preferences. Though the GPC will go a long way toward empowering consumers to efficiently exercise their data rights on the web, and to aid them in navigating an often daunting variety of opt-out-request formats, it unfortunately does nothing to streamline user preferences signals in the app ecosystem, an equally important domain of data collection. Increasingly, companies take aggressive tactics to encourage consumers visiting their websites via a browser to instead download a proprietary app. Reddit, for example, one of the world's twenty most-visited websites, follows visitors across its website with a floating banner that reads "This page looks better in the app" and includes a download button. For a significant

¹² If the agency accepts our recommendation to require that any browser downloaded by California consumers natively support GPC, then this requirement would be less urgent. However, conspicuous links serve a valuable educational function in all cases.

¹³ BestBuy.com. Accessed Nov. 2021 via: <https://www.bestbuy.com/site/california-privacy-rights/do-not-sell/pcmcat1576178819013.c?id=pcmcat1576178819013>

range of businesses, accessing services via an app is the norm, and this trend will only accelerate, given businesses' myriad incentives to coax consumers into the contained environs of a proprietary app, as well as the genuine conveniences these apps offer. The Agency must therefore ensure that consumers are equally empowered to protect their data rights within the app ecosystem as they are on the open web. To this end, the Agency should require that mobile apps solicit *opt-in consent* for the sharing or sale of personal information upon first use of the app.

Recent changes to how Apple's iOS solicits consumer tracking preferences are instructive with respect to the efficacy of an opt-in system. In Spring of this year, Apple began requiring iOS apps to solicit user consent for allowing the app "to track your activity across other companies' apps and websites" via a unique identifier associated with their device. A global device setting also allows iOS users to reject all of these requests by default. The reception of the feature has been illuminating: When presented with the option, 96% of iOS users chose not to allow cross-service tracking.¹⁴ Clearly, consumers choose privacy when given an accessible, easy-to-interpret choice. (However, recent research also suggests the limits of this feature; even when a user has opted-out of tracking, apps have been able to work around this limitation to continue to track individuals.¹⁵) There's an oft-overlooked detail to this story, though. The global setting that allows iOS users to opt out of all cross-service tracking, accessible via the phone's settings menu, was available long before the software update that made it mandatory for apps to display opt-in forms within their apps. In other words, the massive surge in tracking opt-outs that followed the update was not due to a new capability on the part of consumers, but rather to a new presentation of that capability via the user interface.

Though consumer response to the new iOS tracking opt-out is a valuable reference point, the feature is no substitute for a "Do not sell or share my personal information" request as envisioned under the CPRA. iOS' built-in feature prevents cross-service tracking, but it does nothing to limit data collection *within* an app or that data's subsequent use. "Do not sell" requests directed at mobile apps must currently be navigated by consumers without help from the mobile platform provider, and they are often just as hard to find within apps as they are on the web, buried in settings pages or at the end of a labyrinth of links. Until all mobile platforms are required to introduce a mobile analogue to the GPC—a setting that would allow consumers to automatically opt out of the sharing and sale of their personal information gathered directly by apps — the Agency should mandate that companies

¹⁴ Axon, Samuel. "96% of US users opt out of app tracking in iOS 14.5, analytics find."

<https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/>

¹⁵ Geoffrey Fowler and Tatum Hunter. "When you 'Ask app not to track,' some iPhone apps keep snooping anyway".

Washington Post, Sept. 23, 2021. Available at: <https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/ology/2021/09/23/iphone-tracking/>.

approach the exercise of consumer data rights in a way that's already been demonstrated to work: a pop-up dialogue displayed upon first use of the app. We recommend this form give consumers the right to *opt in* to the sale and sharing of personal information as opposed to opting out, or at minimum, that it does not pre-select, highlight or otherwise give biased placement to the option to consent to personal information sales and sharing. Apple's recent experimentation in strengthening user choices around privacy has shown that this method of soliciting consent is effective and that consumers are eager to exercise their rights in this way. The Agency should require businesses to adopt this simple, powerful approach and ensure that consumers are fully empowered to make their own decisions on the sale and sharing of their data when accessing services via apps.

c. What technical specifications should be established for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.

If the Agency accepts our recommendation that any browser downloaded by a California resident both support GPC and have GPC turned on by default, then the sale and sharing of information can only be initiated when a user elects to turn GPC off. In that circumstance, consumers can be presented on a per-business basis with a set of user interface options informing them that: 1) users aged 12 and under may opt-in to selling/sharing only with the affirmative authorization of a parent or guardian; and 2) that users aged 13 and over may opt in directly. We think this would be an improvement over the current set of regulations, which are overly complex, and allow businesses to take advantage of the fact that if a website or app visitor is not known by the business to be under the age of 16, then the business could simply collect information from that visitor as if they were an adult. However, any opt-in user interface elements must be compliant with respect to the dark patterns provisions of the CCPA and the CPRA.

e. What businesses should do to provide consumers who have previously expressed an opt-out preference via an opt-out preference signal with the opportunity to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information.

After the twelve-month opt-out window has passed, a business may ask a consumer directly whether they wish to opt-in to information sale or sharing. We recommend that the Agency provide clear user interface guidelines that demonstrate appropriate methods for initiating this dialogue that prohibit the use of dark patterns (as already articulated regarding consent in the CPRA) or any other design element or language that is deceptive, manipulative, or coercive.

Topic Six: Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information

The following two questions on this topic are addressed, in turn, below:

a. What constitutes "sensitive personal information" that should be deemed "collected or processed without the purpose of inferring characteristics about a consumer" and therefore not subject to the right to limit use and disclosure.

b. What use or disclosure of a consumer's sensitive personal information by businesses should be permissible notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information.

Our interpretation of the two questions above are as follows: a) Are there any contexts in which SPI should be able to be collected and used without being subject to limits on use and disclosure?; and b) Are there any uses or disclosures by businesses that should be allowable regardless of a consumer's expressed preference to limit their use of SPI? In sum, we suggest that precise geolocation data could be collected and processed within a narrow and pre-specified context of use, subject to the limitations we address below.

The section referenced by the relevant footnote to Topic 6(a) is Civ. Code §1798.121(d) which provides for an exception to the opt-out regime for sensitive personal information (SPI).¹⁶ The existing permissible uses of SPI collected from a consumer that are allowed following a consumers exercise of the opt-out right under subsections (a) and (b) are those:

- (1) necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services;
- (2) to perform a limited set of "business purposes" set out in §1798.140(e), namely ensuring the security and integrity of consumer personal information, short-term transient use such as non-personalised advertising (if not disclosed to third parties), operational purposes such as order fulfilment and processing of payments, and quality and safety assurance for services or devices used by the business; and
- (3) as otherwise authorised by regulations enacted under §1798.185(19)(C).

Subsection (19)(C)(iv) of §1798.185, to which §1798.121(d) refers, provides detail in respect to the purpose of any further regulations providing for additional categories of exempted SPI. When read together, §1798.121(d) and §1798.185(19)(C) contemplate the

¹⁶ §1798.121(d) provides that "[s]ensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this act, including Section 1798.100".

making of regulations that identify SPI and contexts of use which is not collected for the purposes of inferring characteristics about a consumer and therefore should be added to those limited permissible uses which apply to SPI even after the relevant consumer has exercised their opt-out right.¹⁷ This is provided that any such permitted uses balance business need and consumer privacy and do not provide a means to circumvent the opt-out protections.

The CPRA introduced the category of sensitive personal information (SPI), we presume, based on the assumption that there are types of information that, irrespective of the context for which it was collected, present a moderate to high risk to individuals should it be disclosed without permission, lost in a breach, or sold to a third party.

Our comments primarily relate to 'precise geolocation' data which has high operational value to businesses providing a number of services and whose use in many contexts is not intended to infer characteristics about the relevant consumer to which that SPI relates. Arguably, there are other types of data, such as one's sequenced personal genomic data, that may carry a similarly high privacy risk and threat of identification or inference, though we limit our discussion here to precise geolocation. Accordingly, we recommend that the Agency consider 'precise geolocation' data as a suitable candidate for inclusion in further statutory exemptions from the right of an individual to limit the use and disclosure of SPI.

While §1798.121(a) currently requires that SPI that is subject to an opt-out request be used only as necessary to perform the relevant service or goods reasonably expected by an average consumer, we believe this limitation is overly broad in the context of 'precise geolocation' data and any permitted uses of such data notwithstanding an opt-out request should be more narrowly tailored. In particular, it is arguable that a 'service' provided to a consumer for which 'precise geolocation' data is allowed to be used may be construed broadly to include a range of ancillary or incidental uses related to the primary purpose for which such information was collected. This is particularly true where an individual profile or account that includes 'precise geolocation' data is applied across a suite of digital services provided by a business.

We continue to emphasize that the risk of inferring characteristics of a consumer based on 'precise geolocation' data remains high and any regulations which contemplate permissible uses of 'precise geolocation' data should address the risk of inferring further

¹⁷ §1798.185(19)(C)(iv) provides that the Agency shall issues regulations with the goal of strengthening consumer privacy while allowing for legitimate operational interests of businesses, including regulations "[e]nsuring that the exemption in subdivision (d) of Section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer, while ensuring that businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information under Section 1798.121".

SPI from use of 'precise geolocation' data, for instance: geolocation attributable to an individual at places of worship, healthcare facilities, or politically meaningful locations or events.

In order for the collection and processing of geolocation data to justifiably be exempt from the broader SPI use/disclosure opt-out limitations, the collection or processing should be: time- and event-limited (i.e. not rolling, aggregated or historical), as well as compliant with any existing data minimization requirements contained within the statute; disclosure to third parties should be prohibited without additional consent regardless of an average consumer's reasonable expectation that such a disclosure might occur; and, individuals should only be locatable at a general (coarse) level of precision.

More broadly, we recommend the Agency consider further regulations in the form of positive obligations on organizations to delete SPI, particularly 'precise geolocation' data, following its time- or event-limited use. Where certain SPI is exempt from the use/disclosure opt-out regime for specific time and event limited purposes, the data minimization obligations in respect to that data should be broader and more onerous. Further regulation may also consider limitations on the cross-referencing of 'precise geolocation' data and biometric identifiers where the risk of attribution to an individual is higher, for instance biometric authentication for payment processing.

Topic Eight: Definitions and Categories

Comment on select questions surrounding the possible update to CCPA- and CPRA-related terms and categories are provided below:

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

"Emotions" or "Emotional state": While §1798.140 (v)(K) includes "preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes" as part of the definition of inferences, given the increasing use of AI to attempt to detect or measure individuals' emotions or emotional state, we recommend that these terms comprise their own category of personal information (and potentially, sensitive personal information).

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

The Agency should consider amending the definition of 'sensitive personal information' (SPI) to address inferences that can be characterized as SPI drawn from non-SPI personal information. These inferences are of concern when they result from the application of data analytics to personal information relating to an individual for the purposes of generating further salable or marketable insights. A revised definition of SPI should contemplate insights which themselves concern or infer a category of SPI about an individual, whether true or not.

c. Updates, if any, to the law's definitions of "deidentified" and/or "unique identifier."

The Agency should consider amending the definition of 'deidentified' to provide further clarity in respect to the reasonableness standard applied to the reidentification risk of anonymized information. The standard should contemplate a rapidly evolving technological and computing environment and, in respect to SPI, require a standard of care commensurate with the inability of an individual to protect themselves against unauthorized disclosure or misuse stemming from reidentification. The Agency should consider imposing a higher standard of care within the definition of 'deidentified' and/or minimum standards and technical guidance on compliant anonymizing treatments.

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

We suggest revisions to either the definition of dark patterns, or to related terms incorporated by reference in order to allow for a broader interpretation of what constitutes a dark pattern. Our concern stems from the fact that the present focus of dark patterns research and taxonomy creation has been with static visual user interfaces. However, emergent technologies may also deploy dark patterns, such as voice activated systems, or other new user-computer interfaces that don't fit the category of traditional static visual user interfaces. Additionally, there are open questions about how to classify dynamic or adaptable user interface mechanisms, such as algorithmically driven content feeds, that foster coercive or manipulative digital interactions that again are not easily described as "user interfaces." Broadening the definition of what constitutes an "interface" would ensure that the regulation can adapt to changes that expand past the traditional graphical user interface. We discuss this topic in greater depth in the paper we reference in the following section on dark patterns.

Topic Nine: Additional Comments

We appreciate the opportunity to provide the Agency with additional comments on the following issues which we think are highly relevant to the scope of the CPRA regulations:

1. Revise the CCPA reporting requirements. The observations in this section are based on ongoing research of the CCPA metrics from 100 companies across industries and sizes.
 - Overall recommendations:
 - Currently, the scale of CCPA reporting metrics are inconsistent across firms, and this makes comparisons difficult to interpret. Some companies elect to expand CCPA rights to U.S. and global user bases, and their CCPA metric reporting include non-Californians. It would be helpful for research purposes if firms explicitly indicated the scope of their implementation of CCPA in their metric reports, or limited their reporting to Californians only.
 - Inconsistencies in reporting the mean versus median response rates to requests make it difficult to compare performance across companies. Having data on both the mean and median will help contextualize the metrics.
 - Some companies are unclear about the timeframe of the reporting, electing to display metrics, for example, from a few months or splitting across two calendar years.
 - Finally, companies subject to reporting requests should be obligated to submit these metrics to the Agency directly, for the Agency to post publicly and track.
 - Access requests:
 - What counts as compliance with access requests is unclear and may vary across companies. Some firms distinguish in their metrics requests where they have provided personal information, as opposed to data categories.
 - Relatedly, most firms do not specify the type of identifiers used to fulfill access requests, which presents a challenge in interpreting the metrics. More specificity along the two dimensions mentioned will enable researchers to better evaluate CCPA's impact.
 - Opt-out requests:
 - Companies have a wide interpretation of what constitutes an opt-out request, making it hard to evaluate corporate compliance using these metrics. First, about one-third of the companies in our preliminary study did not disclose metrics related to opt-out requests. The rationale was that they did not sell the personal information of customers. Second, among the companies that did disclose said metrics, many of them interpreted the opt-out requests pursuant to CCPA as equivalent to users' responses to cookie consent management banners. More research is needed to see whether companies treat cookie banners as substitutes for explicit DNS links.
 - The decision to equate cookie consent preferences and DNS preferences tends to lead to impressive response rates, given cookie

consent forms' scale and automation, and purportedly expands the right to opt-out to all users that visit a website. However, this raises the question of whether corporate responses to consumer cookie preferences sufficiently uphold the right to opt-out under CCPA. The problem is that an individual can opt-out multiple times, and, in cases where their browsers clear cookies after a session, they have to re-assert their choices. This not only leads to double counting in CCPA metrics, but also casts doubt on the efficacy of using responses to cookie consent preferences as a measure for opt-out metrics.

- Equating cookie consents and DNS preferences further does not address how consumers may opt out from the sale of personal information when interacting with firms that enable third-party companies to collect, use and share users' personal information, as defined by CCPA. Furthermore, opting out from a website may not automatically translate into opting out from personal information collected in mobile applications.

2. Dark patterns: The CCPA introduced language targeting specific forms of dark patterns observed in CCPA "Do Not Sell" opt-out requests, while the CPRA includes both a definition of "dark patterns," as well as prohibitions focused narrowly on the use of dark patterns in consent mechanisms related to the disclosure of personal information. Co-Author King argued in a recent paper, *"Regulating Privacy Dark Patterns in Practice—Drawing Inspiration from the California Privacy Rights Act,"*¹⁸ that the current language included in the CPRA presents a model for other states and regulatory agencies to follow. However, much of the possibility that the CPRA offers will be determined by how the Agency intends to regulate this area, and whether it does so expansively or conservatively. We offer the commentary in this article as a reference to the Agency on how to approach further regulation of this topic, and note specifically: "[t]he optimal outcome is not one where consumers are given more checkboxes to check and buttons to click in the name of "compliance." If we are not careful about how we interpret coercion and manipulation, consent mechanisms will merely be fragmented into more rote and meaningless actions rather than transformed into new mechanisms that are more substantive, meaningful, and informative. In prohibiting dark patterns, the CPRA creates an opportunity for California to lead by example and develop standards that demonstrate best practices—or light patterns—for consent."¹⁹

¹⁸ 5 GEO. L. TECH. REV. 250 (2021). Available at: <https://georgetownlawtechreview.org/regulating-privacy-dark-patterns-in-practice-drawing-inspiration-from-california-privacy-rights-act/GLTR-09-2021/>.

¹⁹ Ibid, at 272.

From: Alyssa Doom [REDACTED]
Sent: 11/8/2021 12:46:19 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Keir Lamont [REDACTED]
Subject: [PRO 01-21] CCIA Reply to Invitation for Preliminary Comments
Attachments: [CCIA] CPRA Preliminary Rulemaking Comments.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Dear Ms. Castanon:

Please find attached the Comments of the Computer & Communications Industry 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 (Proceeding No. 01-21).

Sincerely,

Alyssa Doom

—
Alyssa Doom
State Policy Director
Computer & Communications Industry Association
[REDACTED]



**Computer & Communications
Industry Association**
Tech Advocacy Since 1972

Via Electronic Mail (regulations@coppa.ca.gov)

November 8, 2021

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

Re: *Computer & Communications Industry Association comments on proposed rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)*

Dear Ms. Castanon:

Thank you for the opportunity to comment on the California Privacy Protection Agency's ("Agency") preliminary rulemaking activities regarding the California Privacy Rights Act of 2020 ("CPRA").¹ The Computer & Communications Industry Association ("CCIA") is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For nearly fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy.²

CCIA members place high value on the protection of individual privacy and support the important principles that underpin the CPRA including transparency, accountability, and consumer control with respect to data processing practices. CCIA further welcomes the thoughtful and deliberative approach taken by the Agency in seeking comments on critical operational and enforcement issues introduced or modified by the CPRA that are not reflected in the underlying California Consumer Privacy Act ("CCPA") or existing CCPA regulations. The Agency has an important role to play in ensuring that California consumers are fully empowered to understand and exercise their privacy rights and that organizations have sufficient clarity and guidance in order to meet their compliance obligations by the CPRA's effective date.

The following comments reflect high-level observations on the CPRA regulatory process as well as specific responses to topics and questions raised in the Agency's Invitation for Preliminary Comments.

¹ California Privacy Protection Agency, "Invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020" (Sept. 22, 2021), https://coppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

² A list of CCIA members is available at <https://www.cciagnet.org/members>.

I. High-Level Issues for CPRA Regulations

1. Promote Interoperability with Comparable Privacy Regimes

While California has long been a leader in the protection of consumer privacy interests, other U.S. states are increasingly moving to enact their own comprehensive privacy laws and regulatory frameworks.³ Where practicable, the Agency's forthcoming regulations should seek to support consistent interpretation and application of CPRA definitions, rights, and responsibilities with existing industry best practices and comparable regulatory regimes for the protection of consumer privacy. Doing so will help to ensure that Californians are fully protected and empowered to exercise their rights without placing unnecessary compliance costs and duplicative operational burdens on companies or limiting innovation in the data-enabled economy.

2. Preserve Exemptions Enabling Socially Valuable Processing Activities

The CPRA and the underlying CCPA and implementing regulations establish various protections for business activities based on considerations of practicality, the necessity to protect trade secrets and privileged materials, the promotion of privacy enhancing processing activities, and ensuring that certain beneficial data processing activities are not restricted. In considering rulemaking on additional topics directed by the CPRA, it will be important for the Agency to clearly incorporate existing exemptions and carve-outs where applicable. For example, any new regulations should be carefully crafted so as not to interfere with a business's ability to process data for purposes relating to fraud prevention, anti-money laundering, screening, or for other types of activities relating to security, compliance, and legal obligations.

3. Distinguish Human Resources and Business to Business Data

The CPRA, like the CCPA, provides exemptions for data collected in the context of employment and business to business communications.⁴ While these exemptions are currently set to expire in 2023, the CPRA recognizes that there are important differences between these data categories and information collected in the context of the relationship between a business and its customers.⁵ Furthermore, the California legislature is actively working to provide amendments that will address this section. Therefore, CCIA recommends that in the interim, any forthcoming regulation distinguish employee and business to business data so as to avoid prematurely addressing the issue.

³ See Virginia Consumer Data Protection Act ("VCDPA") § 59.1-571 *et seq.* (Mar. 2, 2021) and Colorado Privacy Act ("CPA") § 6-1-1301 *et. seq.* (July 7, 2021).

⁴ CPRA § 1798.145(m) and CCPA 1798.145(n).

⁵ CPRA Sec. 3(A)(8).

II. Responses to Agency Topics

1. Risk Assessments Performed by Businesses

Risk assessments are an important accountability measure that support the protection of consumers' data privacy and security interests. In order to best promote this outcome, any Agency regulations establishing standards for when and how businesses are to conduct risk assessments pursuant to the CPRA should be principles-based, directed towards mitigating reasonably foreseeable risks of substantial harms, and adaptable to the context of different types of products, services, and processing practices.

a. *Criteria for Conducting Risk Assessments*

Privacy and security are intimately related though ultimately distinct concepts in terms of individual risk. Therefore, the Agency should consider promulgating specific, separate guidance for how to assess when the processing of particular information may present a "significant" risk to either consumers' privacy or consumers' security, consistent with emerging U.S. legal standards.⁶ From the perspective of significant risks to security, standards for conducting an assessment should be limited to the processing of data that, if compromised, is likely to result in tangible harm to individuals such as identity theft or fraud, physical injury, or disclosure of objectively sensitive personal details. From the perspective of significant risks to privacy, standards for conducting an assessment should be limited to processing that may produce legal or similarly significant effects to an individual.

Covered businesses conducting risk assessments will further benefit from guidance on their obligations for when to conduct and report risk assessments. Importantly, the regulations should not require organizations to repeatedly reproduce risk assessments for processing activities that have not materially changed and that pose no new or heightened risks. Such a requirement would be operationally burdensome, particularly for small and medium-sized businesses, and could incentivize businesses to treat risk assessments as a mere 'check-the-box' compliance exercise. Where new or significantly changed processing practices present a significant risk, the Agency should establish a reasonable cadence for submitting assessments, such as once per year.

Finally, the regulations should support additional clarity by directly specifying that the "businesses" that must conduct risk assessments are those defined under that CPRA as "determin[ing] the purposes and means of the processing" of the personal information that presents a qualifying risk, and not that business's contractors or service providers.⁷ This is an important clarification because these first-party businesses are best positioned to have the

⁶ See VCDPA § 59.1-576 and CPA § 6-1-1309.

⁷ CPRA § 1798.140(d).

necessary visibility and context to fully evaluate the risks of data processing to all relevant stakeholders.

b. Scope and Content of Risk Assessments

The CPRA directs regulations on risk assessments in instances where processing personal information presents a “significant risk” to consumers’ privacy or security. However, requiring that such risk assessments be conducted with respect to the business’s entire “processing of personal information” would be overly burdensome, likely to result in increased costs to consumers not offset by any benefits to privacy or security protection, and detract from the review of the risk of the actual data and processing practices at issue. Therefore, the Agency’s regulations should provide additional clarity that the scope of risk assessments is limited to the specific processing that presents an identifiable “significant risk” to consumer privacy or security.

The Agency can further support the effectiveness and efficiency of risk assessments by providing additional information on the factors relevant to balancing the benefits of processing against its risks for relevant stakeholders. CCIA recommends that the Agency promulgate regulations recognizing that relevant factors to this analysis may include: (1) technical and organizational measures and safeguards implemented by the business to mitigate privacy and security risks, (2) the reasonable expectations of consumers, and (3) the context of the processing with respect to the relationship between the business and consumers.

The regulations on risk assessments should also adopt an outcome-oriented approach to ensuring that assessments support organizational accountability and Agency visibility into data processing risks and protections. The Agency should avoid the creation of formalistic assessment procedures that would require duplication of prior efforts and add unnecessary costs to businesses. The regulations should therefore recognize that risk assessments are an increasingly common requirement under U.S. and international privacy and data protection laws, and promote interoperability by specifying that the Agency will accept risk assessments that were originally conducted pursuant to a reasonably consistent legal requirement. The regulations should further recognize that a single risk assessment may address a comparable set of processing operations that include similar activities.

Finally, the regulations should include protections to ensure that businesses have the necessary confidence to use risk assessments to fully document and assess processing practices, and are not incentivized to treat their assessments as a defensive measure against potential future litigation. Therefore, in addition to the important carve-out for trade secrets, the regulations should clarify that risk assessments submitted pursuant to the CPRA are confidential and exempt from public inspection and copying under the California Public Records Act and that submitting an assessment to the agency does not constitute a waiver of any attorney-client privilege or work-product protection.

2. Annual Cybersecurity Audits

Cybersecurity audits can be an important tool for supporting the protection of user privacy and security. In establishing regulations to set standards and expectations for conducting audits pursuant to the CPRA where required, we recommend that the Agency leverage existing cybersecurity best practices and certification standards to ensure that consumers and businesses receive the benefits of audits without imposing unnecessary costs. For example, many businesses have existing self-audit mechanisms adhering to contextually appropriate legal frameworks and voluntary industry standards and best practices.⁸ The regulations should recognize that self-audit procedures may meet these standards and affirm that the use of third-party auditors (which would add significant burden and expense to many covered entities) are not required. Where appropriate, the regulations should also permit businesses to rely on cybersecurity audits and certifications maintained by their service providers in meeting these requirements.

3. Automated Decision-making

Any Agency regulations concerning automated decision-making should focus on securing the CPRA's designated statutory protections and rights for consumers with respect to fully automated decisions that have legal or similarly significant effects for consumers, without creating unnecessary restrictions on low-risk systems and tools used to support ordinary, operational business purposes. Therefore, the promulgation of any regulations involving automated decision-making or profiling should consider and incorporate the following principles on terminology and scope, access to meaningful information, and consumer opt-outs.

a. *Terminology*

The approach of specifically regulating “automated decision-making” and “profiling” is an emerging concept under both domestic and global privacy law and accordingly, the terms lack clear, universally accepted legal definitions. Under the CPRA, the terms “automated decision-making” and “profiling” could be interpreted as broadly encompassing a range of low-risk processing activities and basic tools that have proven beneficial for both businesses and consumers, such as spreadsheets, spell-checkers, filtering of unwanted, harmful, or unlawful content, and GPS systems. The adoption of overly inclusive regulatory terminology could impede the use of widely accepted tools that benefit California consumers and businesses alike, slowing down routine business processes by orders of magnitude. Therefore, forthcoming regulations should ensure that businesses shall only be obligated to implement access or opt-out requests

⁸ See e.g., the Payment Card Industry Data Security Standard (“PCI-DSS”), *available at* https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss; the HIPAA Privacy Security and Breach Notification Audit Program, *available at* <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html>; and the Asia-Pacific Economic Cooperation (“APEC”) Privacy Recognition for Processor System (“PRP”), *available at* <https://cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf>.

with respect to fully automated decisions (de-emphasizing the Act’s confusing focus on “technologies”) involving personal information with legal or similarly significant effects.

b. *Access to Information About Automated Decisions*

In considering regulations to further enable consumers to access meaningful information about the logic involved in high-risk automated decision-making processing, the Agency could provide guidance on how to develop notices that contain simple and clear information regarding the purpose of the high-risk automated processing and the source, categories, and relevance of processed information. Logistically speaking, companies should be able to meet obligations related to facilitating access to information about automated decision-making processes through existing website disclosures and transparency notices. Importantly, whether businesses are required to disclose information should be proportionate to the level of risk associated with such decisions, and accordingly, disclosures should only be required in connection with automated decisions that produce legal or similarly significant effects for consumers. Providing disclosures for each type of low risk automated decision would overwhelm businesses with no clear benefit to consumers (for example, imagine if all companies had to disclose a description of how OCR technology works to turn a PDF into an editable, searchable document). Further, any regulations should not require that businesses disclose trade secrets or proprietary information such as algorithm(s) or source code. These types of disclosures are unlikely to provide meaningful protections against risk, are of little practical use to ordinary consumers, and can severely chill innovation.

c. *Opt-Out Rights With Respect to Automated Decisions*

Consistent with emerging U.S. privacy regimes, any Agency regulations establishing opt-out rights with respect to automated decision-making should be limited to fully automated decisions that produce legal or similarly significant effects concerning the consumer.⁹ To provide greater legal certainty, any regulations should specify the categories of use cases that would be implicated here – such as decisions that result in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services. Broader applicability to more low-risk decisions would impede ordinary business activity and diminish the availability and function of personalized consumer services. In instances where high-risk automated decision-making processing is essential for the provision of certain services (i.e., a core benefit/function of the service is its automation), such as in-car safety systems, businesses should be able to demonstrate to consumers supplemental precautions taken instead of offering opt-out options.

4. Audits Performed by the Agency

⁹ See VCDPA § 59.1-573(A)(5), CPA § 6-1-306(1)(a)(I)(C).

The CPRA's contemplation of privacy compliance audits carried out by the Agency beyond its specific and statutorily defined investigative powers will be a unique enforcement authority under U.S. law. CCIA appreciates the Agency's solicitation of comments on this issue, as careful consideration must be given to clearly defining the scope of the Agency's audit authority in order to ensure adherence to foundational standards for fairness and due process that animate the American legal system. We further recommend that the Agency consider using the California Administrative Procedure Act regular rulemaking process to ensure meaningful public input on the establishment of any formal audit procedures.

As an initial matter, CCIA recommends that the Agency's regulations establish a voluntary audit program, under which organizations acting in good faith to adhere to their requirements under the CPRA can request review of certain compliance practices. A requesting business and the Agency could negotiate in advance to establish the scope of the audit, which may be limited to particular practices such as the business's CPRA transparency disclosures or user consent flows, with the aim of ensuring or providing guidance for meeting the CPRA's requirements. In fulfilling the Agency's educational role, anonymized conclusions and insight drawn from the voluntary audit program could be published by the Agency on a regular basis. CCIA encourages the Agency to consider the voluntary audit procedures established by the United Kingdom's Information Commissioner's Office as a model.¹⁰

In considering whether to pursue the promulgation of regulations that would provide for the exercise of compulsory audits, CCIA recommends that the Agency consider the following potential regulatory protections for all stakeholders.

a. Criteria for Selecting Compulsory Audit Subjects

The Agency's regulations should ensure that any selection of businesses for compulsory audits will be conducted in a fair and equitable manner. Regulations establishing criteria for compulsory audits should also provide that the Chief Privacy Auditor must have probable, or at least reasonable, cause to believe that a business has engaged or is engaging in a violation of the CPRA or its implementing regulations that implicates a cognizable risk of harm. Alternatively, audits could be fairly conducted by simultaneously investigating common practices of similarly situated companies.

b. Scope of Compulsory Audits

CCIA encourages the Agency to establish guardrails that will require the Agency to set a clearly defined scope for any compulsory audit prior to its commencement. Audits should be limited to the systems, processes, and staff relevant to a particular identified risk or issue, and the Agency auditor should be constrained from using audits to conduct 'fishing expeditions' into other

¹⁰ Information Commissioner's Office, "A guide to ICO audits" (June 2021), <https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf>.

practices and from issuing findings relating to compliance with non-CPRA statutes. As a matter of practice, the regulations should explicitly exempt attorney-client privileged material, and set a presumption against collecting personal consumer information through an audit unless necessary for accomplishing the purpose of an audit.

c. Compulsory Audit Procedures

Regulated entities will require time to adjust their processing practices and compliance programs to meet their new CPRA obligations. Therefore, the Agency should provide that any compulsory audits will not commence until a reasonable period of time following the formal adoption of final CPRA rules. Furthermore, in order to fully comply with a compulsory audit, companies (especially small and medium-sized enterprises) will have to commit significant internal resources to support the audit process. CCIA recommends that companies should be given reasonable notice in advance of an audit (at least thirty days), and reasonable time to comply with any production, review, interview, or other auditor requests.

The Agency should also ensure the protection of any audit materials by establishing secure methods for storing and exchanging information with an audited business, maintaining access logs for that information, and establishing internal safeguards to ensure that audits operate fully separately from the Agency's enforcement and investigation teams. In order to maintain the privacy of sensitive business (and potentially personal) information, audit materials should be fully exempt from inspection and copying under the California Public Record Act and subject to confidentiality requirements. Furthermore, following the completion of an audit, the Agency should return and permanently destroy materials collected or reviewed as part of the audit process (particularly any personal consumer information).

5. Consumers' Right to Correct Inaccurate Personal Information

The CPRA adopts an important consumer privacy control and brings California into greater alignment with emerging domestic and international privacy standards by creating a consumer right to correct inaccurate personal information.¹¹ In order to ensure the effective and commercially reasonable implementation of this right, CCIA offers the following commentary for the Agency's forthcoming regulations.

First, any right to correct must include appropriate standards for the authentication of requests in order to limit the risk of fraud. CCIA recommends that the Agency adopt similar guidelines to the CPRA's existing verification procedures applicable to comparable requests to access and request the deletion of personal information.¹² However, the right to correct will likely also require new guidance on the establishment of procedures for consumers to provably demonstrate, where appropriate, that the information held by a business is inaccurate.

¹¹ CPRA § 1798.106.

¹² See CPRA § 1798.130.

Second, Agency guidance on the “commercially reasonable efforts” that companies should take in response to a verifiable correction request should recognize that such efforts will be context dependent. Where the presence of inaccurate information may lead to decisions with legal or similarly significant effects to a consumer such as decisions concerning access to credit, housing, or employment opportunities, there should be a higher standard for reasonableness than for information that lacks equivalent impacts.

Finally, the regulations should affirm that the right to correct is limited to objective, factual information that is demonstrably inaccurate. The right to correct should not be interpreted as extending to opinions, inferences, or conclusions which are protected by First Amendment principles for free expression.

6. Opt-Out Preference Signals

The implementation and adoption of opt-out signals is an area with significant uncertainty where the Agency is well-positioned to provide important technical and operational guidance through the regulatory process. CCIA recommends that the Agency develop regulations focused towards: (1) mitigating potential harms to competition by the selective development or deployment of opt-out signals for the purposes of unfairly disadvantaging other businesses, (2) enabling users to simply exercise a choice to opt-in or reverse any opt-out decision, (3) providing guidance on the circumstances under which a business that chooses to allow consumer opt outs through preference signals consistent with CPRA § 1798.135(b)(1) may ignore an opt-out signal and how to respond to multiple, conflicting signals. As the development of opt-out signals may significantly impact diverse stakeholders in the broader Internet ecosystem, we further recommend that the Agency solicit broad input on signal specifications through the upcoming “informational hearings” series.

7. Definitions

CCIA offers the following comments on definitions under the CPRA.

a. *“Deidentified” Information*

In establishing exceptions and carve-outs for data maintained and processed in less identifiable formats, the CPRA incentivizes more privacy preserving data processing practices. Regulations focused on clarity, compliance interoperability, and implementability for these categories of data will best support the widespread adoption of privacy supporting technologies. For example, with “deidentified” data, CCIA recommends that forthcoming regulations remove the confusing reference to “infer[ring] information” and add a requirement that deidentified data also cannot reasonably be linked to a specific consumer’s device, in order to better align this definition with the widely accepted U.S. standard rooted in the Federal Trade Commission’s 2012 report on

Protecting Consumer Privacy in an Era of Rapid Change.¹³ The Agency should further incentivize the use of privacy protective technologies by clarifying the distinction between deidentified and “pseudonymised” data under the CPRA and exempting demonstrably pseudonymized data from data subject requests, consistent with emerging U.S. legal standards.¹⁴

b. *“Precise Geolocation” Information*

The CPRA recognizes that depending on context, location data can be a sensitive category of personal information that may benefit from heightened privacy protections. The Act further establishes a strong standard for the precision of qualifying location information that goes beyond comparable state and federal privacy frameworks that can also be consistently engineered by regulated businesses.¹⁵ Therefore, CCIA recommends that the Agency refrain from seeking to establish any new brightline rules expanding the scope of geolocation information that is considered “precise” based on any single factor such as the density of an area, which could create significant operational burdens for businesses and not necessarily increase consumer privacy protections as there are multiple technical and contextual factors relevant to the precision of location information.

The Agency’s forthcoming regulations can also further define “precise geolocation information” in accordance with the CPRA’s intent and in support of interoperability with comparative legal regimes by (1) specifically carving out from the definition the content of communications, (2) providing that precise geolocation data is reasonably linkable to an identified or identifiable natural person (exempting de-identified and anonymous data), and (3) carving out certain data practices involving location data that are not used to track individual consumer movements over time, such as a consumer’s entry into or exit from a geo-fence used solely for triggering certain desired notifications.

c. *“Specific Pieces of Information Obtained from the Consumer”*

Consistent with the need for operationalizable CPRA requirements and in service of ensuring that consumers are able to obtain useful and actionable information when exercising their access requests, CCIA recommends that the Agency promulgate rules concerning the definition of “specific pieces of information obtained by the consumer.” In particular, the regulations should exclude non-human readable data and information that is stored solely on a client-side or user device beyond the access of regulated businesses.

¹³ Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change” (Mar. 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> see also VCDPA § 59.1-571 and CPA § 6-1-1303(11).

¹⁴ See VCDPA § 59.1-577(B), CPA § 6-1-1307(3),

¹⁵ See VCDPA § 59.1-571 (“‘Precise geolocation data’ means information... that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet.”), Children’s Online Privacy Protection Rule § 312.2 (“Geolocation information sufficient to identify street name and name of a city or town”).

d. *“Dark Patterns”*

The CPRA definition of user interface design features referred to as “dark patterns” is vague and appears to be unworkable in practice. Any user interface that creates structure by establishing a user-flow experience could be interpreted as having the effect of limiting user “choice” to the options that are provided. Providing users with neutral “choice” over the full universe of theoretically possible options and controls would be impractical if not impossible for businesses and consumers alike. For example, the definition would appear to consider defaults set to the most privacy preserving options as “dark patterns” because they would “impair” consumer “choice” and “decision-making” as to their privacy options.

The Agency’s forthcoming regulations should support clarity for this novel legal requirement by specifying the definition of “dark patterns” is focused on deceptive or manipulative design practices that amount to consumer fraud in the contexts where such practices are specifically forbidden under the CPRA. The Agency should further consider engaging with relevant stakeholders, including user-interface designers, with the aim of developing actionable guidance such as examples of prohibited dark patterns and principles of good design, to help guide companies in developing effective and context-appropriate experiences for their users.

Thank you again for the opportunity to comment on the California Privacy Protection Agency’s preliminary rulemaking activities regarding the California Privacy Rights Act. If you have any questions regarding these comments and recommendations, please contact Alyssa Doom at [REDACTED].

Sincerely,

Alyssa Doom
State Policy Director
Computer & Communications Industry Association

From: Katie McInnis [REDACTED]
Sent: 11/8/2021 12:52:13 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: DuckDuckGo CPRA comments 11.8.21.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Dear Sir or Madam,

Please find the comment from DuckDuckGo attached to this email.

Best,

Katie McInnis (she/her)

Senior Public Policy Manager US
DuckDuckGo | Privacy, simplified.



Duck Duck Go, Inc.
20 Paoli Pike • Paoli, PA 19301, United States
+1 267.690.7758 • duckduckgo.com

Katie McInnis

Senior Public Policy Manager, US
Washington, DC

November 8, 2021

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

regulations@coppa.ca.gov

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

DuckDuckGo, a privacy technology company that helps consumers stay more private online, appreciates the opportunity to submit comments on the proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA). We thank the California Privacy Protection Agency (CPPA) for seeking input from stakeholders on the rulemaking process.

We believe that privacy is a human right and that getting privacy online should be simple and accessible to everyone. Therefore, our comment focuses on (1) ensuring that consumers can easily exercise their right to opt-out under the California Privacy Rights Act via a browser-based signal, (2) highlighting how dark patterns of design can undermine consumer choice and control, and (3) urging strong enforcement of the California Privacy Rights Act. DuckDuckGo also broadly supports comments from civil society, like those from the Electronic Frontier Foundation and Consumer Reports.

Section 5: 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

Although the provision of privacy rights to consumers is important, meaningful use is equally important.



Research from California¹ and the European Union² demonstrates how hard it can be for consumers to exercise their privacy rights if they lack an easy way to signal their preferences. To ensure that individuals could easily exercise their privacy rights, DuckDuckGo joined with privacy researchers, advocates, and publishers to create a “Do Not Sell” specification designed to work with the California Consumer Privacy Act (CCPA), which is referred to as [Global Privacy Control](#) (GPC).³ Technology companies have implemented the GPC in their software code and a range of major publishers comply with GPC as a valid mechanism for Californian consumers to opt out of the sale of their personal information under the CCPA.⁴ We urge the CPPA to build on the work by the California Attorney General’s Office under the CCPA by writing rules clearly stating that companies must comply with opt-outs sent via a browser signal.⁵

Section 8(j): Dark Patterns

Dark patterns of design have been and continue to be used by companies to subvert consumer autonomy, control, and choice by steering, pushing, or nudging a consumer towards decisions that allow the company to maximize their ability to extract revenue from consumers. As our attached comment to the Federal Trade Commission demonstrates,⁶ dark patterns can be used by companies to support a range of business considerations from extracting data from users to steering consumers away from competitor services. Therefore, we encourage the CPPA to craft clear rules on the use of dark patterns, building on

¹ Consumer Reports conducted a study with Californian participants to examine opt-outs under the California Consumer Privacy Act. Their research found that consumers often found it difficult to locate Do Not Sell links on data brokers’ homepages and many opt-out processes were onerous enough to impair a consumer’s ability to opt out. Maureen Mahoney, *California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?*, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

² Following the passage of the European Union’s General Data Protection Regulation (GDPR), researchers found that dark patterns in the design of cookie consent notices “substantially affect people’s consent behavior.” Many cookie consent dialogs “offered no meaningful choice to consumers.” Therefore, the report concludes, “our findings demonstrate the importance for regulation to not just require consent, but also provide clear requirements or guidance for how this consent has to be obtained in order to ensure that users can make free and informed choices.” Christine Utz, Martin Degeling, *et al.*, *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (Nov. 2019), <https://doi.org/10.1145/3319535.3354212>.

³ *Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights*, GLOBAL PRIVACY CONTROL (Oct. 7, 2020), <https://globalprivacycontrol.org/press-release/20201007.html>.

⁴ *GPC Privacy Browser Signal Now Used by Millions and Honored by Major Publishers*, GLOBAL PRIVACY CONTROL (Jan. 28, 2021), <https://globalprivacycontrol.org/press-release/20210128>.

⁵ For more on Global Privacy Control, please see the subsection entitled “The CPPA should clarify that compliance with global privacy controls is mandatory under the CPRA” of Consumer Reports’ comments to the Agency.

⁶ See Appendix I.



the work of the California Attorney General.⁷

Section 9: Additional Comments

DuckDuckGo urges the CPPA to strongly enforce the CPRA and the rules the Agency adopts under the CPRA. The implementation of other privacy laws, like the General Data Protection Regulation,⁸ demonstrates that, without proper enforcement, laws can transform into paper tigers, thus failing to protect consumers despite strong rules on the books.

DuckDuckGo thanks the California Privacy Protection Agency for the opportunity to provide feedback on the Agency's proposed rulemaking. We are available to answer questions you have about our submission.

Sincerely,



Katie McInnis
Senior Public Policy Manager, US

⁷ Attorney General Becerra Announced Approval of Additional Regulations that Empower Data Privacy under the California Consumer Privacy Act, CALIF. ATTORNEY GENERAL (Mar. 15, 2021), <https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-additional-regulations-empower-data>.

⁸ Chris O'Brien, *EU report finds GDPR enforcement inadequate in its first two years*, VENTURE BEAT (June 24, 2020), <https://venturebeat.com/2020/06/24/eu-report-finds-gdpr-enforcement-inadequate-in-its-first-2-years/>.



Appendix I

May 26, 2021

US Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Re: *FTC-2021-0019, Bringing Dark Patterns to Light: An FTC Workshop*

Dear Sir or Madam:

Following the April 29, 2021, virtual workshop on dark patterns, we respectfully submit this comment to the Federal Trade Commission, urging an examination of how dark patterns can be used anticompetitively. Specifically, our comment responds to the sixth topic posed by the FTC: Harms of Dark Patterns.

Dark patterns can be and have been wielded by companies to increase their market power. These designs can be used to maximize a company's ability to extract revenue from consumers or to steer consumers away from competitor services or providers. In both instances, consumer autonomy, control, and choice are undermined in the name of market dominance. How dark patterns affect competition in the market is understudied,⁹ and we urge the FTC to examine dark patterns for anticompetitive effects.

How Dark Patterns Are Used to Extract More Revenue from Consumers

Companies use dark patterns to maximize their ability to extract revenue from consumers. This revenue could be in the form of increased purchases but often is in the form of data. As the US House Antitrust Subcommittee report, *Investigation of Competition in Digital Markets*, notes, "the accumulation of data can serve as another powerful barrier to entry for firms in the digital economy" because access to data allows companies to target advertising, improve services, and identify and exploit new market opportunities.¹⁰

⁹ "The dark patterns literature has only provided limited commentary about competition concerns emerging from dark patterns." Arunesh Mathur, Jonathan Mayer, & Mihir Kshirsagar, *What Makes a Dark Pattern...Dark?*, CHI CONF. ON HUMAN FACTORS IN COMPUTING SYSTEMS (2021), <https://doi.org/10.1145/3411764.3445610>.

¹⁰ *Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations*, SUBCOMM. ON ANTITRUST,

Cognizant of the benefit consumer data brings, companies often use dark patterns in consent dialogs or in the privacy settings they provide to consumers. By using dark patterns in consent dialogs or privacy settings, companies are able to extract as much data as possible from consumers while appearing to give consumers control over their data.

Dark Patterns in Consent Dialogs

Companies use dark patterns in cookie consent dialogs to maximize the amount of data they can extract from users by “increas[ing] the likelihood of users consenting to tracking.”¹¹ The House Antitrust Subcommittee report notes this tactic has “become a pervasive tool.”¹² These dark patterns are designed to not only subvert consumer choice, but also render consumer rights enshrined in law difficult to use or unusable.

For example, following the passage of the European Union’s General Data Protection Regulation, researchers found that dark patterns in the design of cookie consent notices “substantially affect people’s consent behavior.”¹³ Many cookie consent dialogs in their research “offered no meaningful choice to consumers”¹⁴ due to dark patterns. Therefore, the report concluded, “our findings demonstrate the importance for regulation to not just require consent, but also provide clear requirements or guidance for how this consent has to be obtained in order to ensure that users can make free and informed choices.”¹⁵

Dark patterns have also been used to undermine US consumers’ privacy rights in California. Consumer Reports found that dark patterns “significantly undermined consumers’ ability to opt out” of the selling of their personal information, a right created by the California Consumer Privacy Act.¹⁶ Echoing the

COMMERCIAL, & ADMIN. LAW OF THE COMM. ON THE JUDICIARY (Oct. 6, 2020), https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.

¹¹ *Id.*

¹² *Id.*

¹³ Christine Utz, Martin Degeling, *et al.*, (Un)informed Consent: Studying GDPR Consent Notices in the Field, PROCEEDINGS OF THE 2019 ACM SIGSAC CONFERENCE ON COMPUTER & COMMUNICATIONS SECURITY (Nov. 2019), <https://doi.org/10.1145/3319535.3354212>.

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ Maureen Mahoney, *California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?*, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

researchers in the EU, Consumer Reports also called for regulators to “more clearly prohibit dark patterns” to “make it easier” for consumers to opt out.¹⁷

By successfully coercing a consumer’s consent or making it hard or impossible to opt-out of the selling of one’s data, companies are able to collect more data from consumers, which benefits their position in the market. These dark patterns are, thus, not just antiprivacy but also anticompetitive.

Dark Patterns of Design in Privacy Settings

Companies like Facebook and Google use privacy-intrusive defaults and dark patterns in consumer-facing privacy settings to maximize the amount of data they can extract from users.¹⁸ Most users do not change default settings, so privacy-intrusive defaults allow companies to extract data from users without friction.¹⁹ However, some users will change their defaults, so companies also employ dark patterns in design to ensure that it is difficult to do so.

A 2018 report²⁰ from the Norwegian Consumer Council (NCC) demonstrates how Facebook and Google create an illusion of consumer control over the consumer’s data while simultaneously nudging and manipulating users into making choices that limit that control. The NCC found that most of the privacy protecting settings that Facebook and Google provide users are disabled by default and changing those defaults can take as many as 13 clicks for the user. As the report notes:

By giving users an overwhelming amount of granular choices to micromanage, Google has designed a privacy dashboard that, according to our analysis, actually discourages users from changing or taking control of the settings or delete bulks of data. Simultaneously, as noted above, the presence and claims of complete user control may incentivize users to share more data.

¹⁷ *Id.*

¹⁸ Geoffrey Fowler, *Hands off my data! 15 default privacy settings you should change right now*, WASH. POST (June 1, 2018), <https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/hands-off-my-data-15-default-privacy-settings-you-should-change-right-now/>.

¹⁹ Lena V. Groeger, *Set It and Forget It: How Default Settings Rule the World*, PROPUBLICA (July 27, 2016), <https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world>.

²⁰ *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (June 27, 2018), <https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/>.

By successfully pushing consumers away from changing defaults or from using data collection and privacy controls, companies are able to collect more data from consumers, which benefits their position in the market.

These dark patterns of design are anticompetitive as well as antiprivacy. Indeed, the ability of these companies to continuously extract more consumer data without inciting a backlash from consumers who want better protections over their data is a sign of their market dominance:

The persistent collection and misuse of consumer data is an indicator of market power in the digital economy. [...] The best evidence of platform market power therefore is not prices charged but rather the degree to which platforms have eroded consumer privacy without prompting a response from the market. As scholars have noted, a platform's ability to maintain strong networks while degrading user privacy can reasonably be considered equivalent to a monopolist's decision to increase prices or reduce product quality. A firm's dominance can enable it to abuse consumers' privacy without losing customers. In the absence of genuine competitive threats, a firm offers fewer privacy protections than it otherwise would. In the process, it extracts more data, further entrenching its dominance.²¹

Without an intervention against these dark patterns of design or a general privacy law restricting what information companies can collect, consumers will be forced to share private information with big companies like Google and Facebook or else cease using their services entirely. In this take-it-or-leave-it environment where consumers also lack the necessary information to compare companies' privacy practices, consumers are left with little, if any, tools to control the sharing of their information. Thus, consumers' control over the privacy of their data is, in this market-dominated context, illusory because the consumer is being actively persuaded to not even use the weak tools provided to them.²² As Professors Gregory Day and Abbey Stemler posit in their forthcoming article *Are Dark Patterns Anticompetitive?*, "the concept of behavioral autonomy may soon become a reflection of market quality, given the dangers of online manipulation."²³

²¹ *Investigation of Competition in Digital Markets*, *supra* note 10.

²² Work from the Norwegian Consumer Council and Consumer Reports demonstrates how weak these controls are. See *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMERS COUNCIL (June 27, 2018), <https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/> and Katie McInnis, *Consumers Union urges FTC to examine Facebook privacy controls, citing new CU research*, CONSUMER REPORTS (June 27, 2018), https://advocacy.consumerreports.org/press_release/consumers-union-urges-ftc-to-examine-facebook-privacy-controls-citing-new-cu-research/.

²³ Gregory Day & Abbey Stemler, *Are Dark Patterns Anticompetitive?* ALA. LAW REV. forthcoming (Oct. 11, 2019), <https://www.law.ua.edu/lawreview/files/2020/11/1-DayStemler-1-45.pdf>.



How Dark Patterns Steer Consumers Away from Competitors

Dark patterns can be and have been used by market dominant actors to steer consumers away from competitors, thus benefiting a company's access to data and position in the market. For example, the House Antitrust Subcommittee report details how Google used a dark pattern to prompt users to "Add Google Meet video conferencing" to an event on Google calendar to nudge users away from competitor video conferencing services from companies like Zoom. As the report notes, this dark pattern was introduced only when remote work became commonplace due to the COVID-19 pandemic and Zoom emerged as the market leader in video conferencing.

Companies also use dark patterns to introduce friction as a way of steering consumers away from competitors. For instance, Google search is the default search engine on Android mobile devices. To change the default search engine to another provider, the user must make more than 15 clicks.²⁴ This fact, combined with the reality that most consumers do not change their defaults, means that only highly motivated users will be able to make the switch. Dark patterns in privacy settings, therefore, affect not only the consumer's ability to protect their privacy but also use to competitor services. These competitor services may also provide the user with better privacy protections if the user is switching to a privacy-protective search engine like DuckDuckGo. The extent to which dark patterns have been used to steer consumers away from competitors is understudied but significantly affects the ability of new entrants to enter the market and compete on privacy.

Thank you for this opportunity to respond to the Commission's request for comments following the workshop.

Sincerely,



Katie McInnis
Senior Public Policy Manager US

²⁴ *Dear Google: We Agree Search Competition Should Be "Only 1 Click Away"—So Why Is It 15+ on Android?*, DUCKDUCKGO (Oct. 14, 2020), <https://spreadprivacy.com/one-click-away/>.

From: Melissa O'Toole [REDACTED]
Sent: 11/8/2021 1:27:23 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Seren Taylor [REDACTED]
Subject: PIFC Preliminary Comments for CPPA Attn: Debra Castanon
Attachments: PIFC Preliminary Comments for CPPA 11-8-21 .pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Good afternoon,

Attached, please find the Personal Insurance Federation of California (PIFC) preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 . If you have any questions regarding PIFC's comments, please contact Seren Taylor at [REDACTED] or [REDACTED]

Thank you,

Melissa O'Toole
Legislative and Communications Manager
Personal Insurance Federation of CA

[REDACTED]
W: www.pifc.org

[REDACTED]
1201 K Street, Suite 950
Sacramento, CA 95814





Date: November 8, 2021

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

Members:

STATE FARM

LIBERTY MUTUAL

PROGRESSIVE

MERCURY

NATIONWIDE

FARMERS

ALLSTATE

Associate Members:

NAMIC

CHUBB

CONNECT

by American Family

SUBJECT: INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING UNDER THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020 (Proceeding No. 01-21)

Dear Members of the Board,

The Personal Insurance Federation of California (PIFC) is a statewide trade association that represents seven of the nation's largest property and casualty insurance companies (State Farm, Farmers, Liberty Mutual Insurance, Progressive, Mercury, Nationwide and Allstate as well as associate members CHUBB, CONNECT by American Family Insurance, and NAMIC) who collectively write the majority of personal lines auto and home insurance in California.

We greatly appreciate the opportunity to provide preliminary thoughts and comments to the California Privacy Protection Agency ("Agency") as you begin the important work of implementing Proposition 24, The California Privacy Rights Act of 2020 ("CPRA") and the California Consumer Privacy Act of 2018 ("CCPA").

For purposes of background, we believe it is important to understand that insurance is a highly regulated industry in general and particularly so in California. The state's Insurance Commissioner heads the largest consumer protection agency in the United States with over 1300 staff and a \$300 million budget. Current law provides the commissioner with unrestricted access to the records, employees, officers, and contractors of any insurer. The commissioner is required to investigate the compliance of an insurer (commonly referred to as a "market conduct examination") periodically (generally every five years) but is permitted to examine an insurer at any time. Notably, insurers must reimburse the commissioner for the costs incurred conducting an examination. Few industries have the routine presence of a regulator with the power of the Insurance Commissioner.

Regarding the specific topics and questions the Agency has formulated to frame discussion, PIFC respectfully submits the following general comments to help inform future work. These are intended to be insurance industry specific comments that should be considered in addition to the comments the Agency will receive from the broader business community, which also reflect input from insurers.

Cybersecurity Audits & Assessments

- To the extent that CPRA requires cybersecurity audits or consumer privacy risk assessments:
 - The Agency should strongly consider the fact that Insurers are already regulated under the Insurance Code and the Financial Code because they are subject to plenary audit authority by the CDI.
 - To the extent insurers perform cybersecurity audits as required by other laws/regulations or do so as an industry best practice they should be deemed in compliance with any California requirements.
 - Additionally, any audits or assessments should be standardized to conform to industry recognized cybersecurity standard and should mirror, or otherwise harmonize with, other cybersecurity audits or assessments required by California law.

Automated Decision-Making (ADM) Technology

- To the extent that CPRA regulates automated decision-making technology:
 - When the Agency enters formal rulemaking, it will be very important to recognize current State and Federal regulations that already regulate ADM to avoid duplication or conflicting regulations for insurers.
 - ADM technology regulations should not impose any bans or purpose limitations on insurers use of artificial intelligence/machine learning; or to the extent this is not possible, bans or purpose limitations should not be unduly burdensome on insurer operations or efforts to innovate.
 - Innovative technology has its benefits for businesses, and we request the Agency focus any regulation on ADM that impacts individuals as opposed to ADM that helps a business run more smoothly (e.g., like a call router).
 - Insurers or insurance-related activities such as rating should be exempt from the California law's definition of profiling. Including such activities in profiling may have a negative impact on the ability of insurers to deliver affordable products to California consumers.
 - If ADM is applied to the business of insurance, clarification is needed as to what is meant by the term (i.e., in the Claims world, if certain medical bill processing software is deemed "automated decision making" and consumers have a right to opt-out, that could quickly become a problem and have an enormous operational impact. At a minimum, allowing opt-outs of that nature would delay claim handling timeframes (to the detriment of the claimant) and compromise insurers' ability to timely comply with various Fair Claim Settlement Practice Regulations.
 - Additionally, we would appreciate clarity on how trade secrets and proprietary information would be protected, should regulations require audits or transparency.

For insurers, the challenge of multiple regulators promulgating regulations, examining conduct, and taking enforcement actions is significant. With these preliminary insurance industry specific comments, PIFC is hopeful that the Agency will recognize the existing state and federal rules that insurers already comply with, and that avoiding unnecessary, duplicative, and conflicting regulations will be a core principle. Given the complexity and cost of compliance with CPPA and CPRA, our members also seek flexibility wherever possible and appropriate. We look forward to working collaboratively with the Agency and Board to develop fair regulations that can be implemented in a manner that best serves Californians.

Sincerely,



Seren Taylor
Senior Legislative Advocate

From: Crenshaw, Jordan [REDACTED]
Sent: 11/8/2021 1:37:33 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 Comments for US Chamber of Commerce on CPRA
Attachments: U.S. Chamber of Commerce California Privacy Rights Act Comments 11-8-21.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

To Whom It May Concern:

Please find the U.S. Chamber of Commerce's comments regarding the CPPA's request for comments on the California Privacy Rights Act.

Please let me know if you have any questions.

Best,

Jordan Crenshaw

Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce
Direct: [REDACTED] Cell: [REDACTED]



U.S. Chamber of Commerce

www.americaninnovators.com

@uschambertech



JORDAN CRENSHAW

Vice President

1615 H STREET, NW
WASHINGTON, DC 20062-2000

November 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)

In response to the California Privacy Protection Agency's invitation for preliminary comments, the U.S. Chamber of Commerce Technology Engagement Center ("C_TEC" or "Chamber") appreciates the opportunity to provide comments regarding the proposed rulemaking under the California Privacy Rights Act ("CPRA"). Although the business community asserts it is imperative that Congress pass a national privacy law that protects all Americans equally, it is also important that California's Privacy Protection Agency ("Agency" or "CPPA") effectively implements the CPRA and create certainty for consumers and businesses

Businesses need clarity to facilitate compliance with the regulations. Additionally, the CPPA should give companies adequate lead time to implement compliance programs and practices before rules are enforced.

The Agency should, where feasible and appropriate, work to align the requirements of CPRA with other state privacy laws to encourage better compliance and uniformity. The Chamber also encourages the Agency to facilitate permanent exemptions for employee and business-to-business information.¹

In response to the Agency's specific regulatory requests, the Chamber offers the following comments organized by question number for your consideration.

¹ CPRA exemption for employee and business-to-business data sunsets January 1, 2023. To the extent the legislature does not extend or make permanent these exemptions as of this date, the CPPA will need to provide clarifying guidance at that time. For example, a business should not be required to correct information about an employee if such information is based on a legal document (e.g. green card, passport, name change decisions) that the employer holds about that employee.

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

To promote greater uniformity nationwide and ease compliance, the Chamber suggests harmonizing approaches with those undertaken in Virginia and Colorado.

As drafted, it is unclear what would constitute a “significant risk” and therefore trigger an audit and assessment. It is suggested that the Agency clarify the definition of “*significant risk to consumers' privacy or security*.” To ensure that audits and assessments meaningfully enhance consumer privacy, The definition should be focused on mandating audits and assessments for processing that involve a substantial and identifiable risk of harm to consumers.

For the cybersecurity auditing requirements, the regulations should follow a risk-based approach. Businesses may be required to certify that they have implemented and adhere to policies and procedures designed to secure that personal information whose dissemination would present the greatest risk for the consumer's privacy or security. Any new requirements should be consistent with California's existing data security requirements, as established in [Cal Civ. Code § 1798.81.5](#). Businesses should be permitted to leverage existing industry standards certifications to make this process less onerous. This includes the ISO 27000 series certification, conformity with the NIST Cybersecurity Framework, the annual Payment Card Industry merchant certification, Service Organization Control audits by internal and third parties, and/or security programs established pursuant to consent decrees with regulators such as the FCC or FTC. Businesses should be permitted to select qualified, independent third-party auditors of their choice. Moreover, the regulations should also permit internal audits, provided that there are structures in place to ensure that any internal audit can remain both thorough and independent. The option for an internal audit will be critically important for SMEs, which likely will not have the sources for the burden and expense of independent third-party audits.

For the risk assessment requirement, a business that has completed and submitted a risk assessment, a business should not be required to perform additional risk assessments. Moreover, the regulations should expressly acknowledge that the scope of a risk assessment is limited to the specific processing activity or activities that trigger the requirement under the “significant risk” definition. This will focus the assessments on enhancing consumer privacy protections while balancing effective oversight by the Agency.

The CPPA will be overwhelmed if it requires the constant submission of risk assessments. Instead, the regulations should give the Agency the power to request risk assessments when they are relevant to an investigation or inquiry. These assessments should be confidential, and the rules should recognize that privileged information or trade secrets will be redacted. This will help protection company intellectual property as well as consumer personal information contained in the report. The Agency should ensure that the assessments cannot be revealed through California's Public Records Act and should not be made public.

2) Automated Decisionmaking - The CPRA provides for regulations governing consumers’ “access and opt-out rights with respect to businesses’ use of automated decisionmaking technology.”

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

The use of innovative technologies, such as automated processes and technologies, benefit businesses tremendously, allowing them to increase productivity, prevent and detect fraud and identity theft, improve business processes, save costs, better allocate resources, and better use the talents of their employees. As the Agency looks at what should be deemed an “automated decisionmaking technology,” C_TEC encourages the Agency to take a risk-based approach, focusing not on technologies, but on the circumstances where those technologies have a significant, direct, tangible impact on either the economic or legal rights of the consumer. Any rules should not apply to inconsequential decisions made by automated decision technology.

Furthermore, C_TEC would encourage the CPPA to review current State and Federal regulations that already regulate automated decisionmaking technologies. Potentially deeming those already regulated industries within the scope of the CPRA could possibly cause unnecessary duplication of rules for businesses. Moreover, we encourage the CPPA to consider other domestic and international questions this rulemaking will raise. This includes how to harmonize with any federal requirements and frameworks. It also includes the recent EU-US pledge to collaborate on a common framework for the protection of human rights in AI at the summit for the recently launched Trade and Technology Council. Finally, we would encourage the Agency to make any regulation flexible to allow for future refinements.

b. When consumers should be able to access information about businesses’ use of automated decisionmaking technology and what processes consumers and businesses should follow to facilitate access.

C_TEC would encourage that any CPRA rulemaking indicates that the information should be presented upfront to the consumer in a disclosure (e.g., privacy policy) that will provide necessary information regarding the businesses’ use of “automated decisionmaking technology.” Furthermore, we believe consumers should be able to use the same self-service portals or other methods by which they currently exercise rights under the CPPA or other sector-specific regulations.

c. What 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.

C_TEC encourages CPPA to leverage existing NIST principles, including the recently finalized “Four Principles of Explainable AI”, to provide aligned guidance with what businesses must do to provide “meaningful information about the logic” involved in the automated decision-making process. Meaningful information about the logic should be focused on high level controls

that support explainability, transparency, robustness, and trustworthy AI principles. The actual logic of the model is proprietary and should remain so.

C_TEC believes that it is essential to highlight that general access and correction rights are already provided to consumers within CPRA and required in many other sector-specific regulations.

d. The scope of consumers' opt-out rights with regard to automated decisionmaking, and what processes consumers and businesses should follow to facilitate opt outs.

C_TEC would encourage any substantive expansion of opt-out rights in the CPRA to be adopted by the legislature rather than through an administrative rulemaking procedure. The core of California privacy law is the opt-out right, which is clearly defined in statute and has been subject to voter approval. The ambiguous provision in the rules regarding opt-out rights and automated decisionmaking does not support the creation of new duties and rights, which further expands the newly amplified opt-out right.

If any new rules regarding opt-out must be adopted, personal information protected under other financial privacy laws (federal or state) should continue to be excluded from the scope of this specific opt-out request. As well as an exemption for when an opt-out may cause harm or adverse impact to consumer out – e.g. packet routing – opt-out could slow down internet speed. Finally, and an exemption should be put in place for when an opt-out request is not feasible – e.g. a non-automated decision system cannot accomplish the task.

Furthermore, if the CPPA moves forward with an opt-out right tied to automated, decision-making, we would highly encourage it to follow the General Data Protection Regulation; consumers may opt-out of solely automated decisionmaking by requesting a human review of a decision that has caused a significant, direct, and tangible impact. Allowing consumers to opt-out of any automated process involving consumer data that leads to an insignificant decision (e.g., the decision to recommend one tv show over another on a streaming service) has the potential to cause disruption and inefficiencies for businesses without providing a commensurate benefit to consumers.

3) Audits Performed by the Agency

The Agency should perform an audit only where there is evidence that a business has misused personal information or violated substantive provisions of the CPRA, creating either harm or a substantial risk of harm to consumers. For example, a company that is honoring a consumer's "Do Not Share" wishes but whose sole failure under CRPA is not proving a "Do Not Share" button should not trigger an audit without other negative circumstances. The rules should require a majority of Agency members to vote in favor of an audit before one can be ordered and to issue a resolution that cites the relevant evidence and defines the scope of the audit being required. The scope should be limited to addressing practices directly related to the misuse of personal information that gave rise to the audit. The Agency might follow the lead of the Federal Trade Commission and require audits to be performed after the end of an enforcement action against a business.

The CPRA should give a business the option to select an independent, certified auditor to perform any audits. (Regulations must also ensure the protection of businesses' proprietary information disclosed during the audit.)

Because audits can and do result in a finding of no material deficiencies, the agency should ensure that any audits contain robust confidentiality/proprietary safeguards so that an audit cannot be revealed to the public through California's Public Records Act. Additionally, the data, algorithms, and other proprietary material that the agency is authorized to review should receive similar confidentiality/proprietary protections.

4) Consumers' Right to Delete, Right to Correct, and Right to Know

Responding to Requests

The Agency should provide clarification on the requirement for businesses with a physical presence to have a toll-free phone number allowing consumers to exercise their privacy rights. Some companies have a very small physical presence in which all users are funneled through an app or other online means, making their requirement for a staffed toll-free number an extremely burdensome and highly unnecessary one.

In responding to consumer requests, businesses should not be required to take extra steps (beyond what's required today under the CCPA) to identify a consumer whose identity is unknown to the business. This would represent a disproportionate effort.

Right to Correction

The CPRA specifies that the right to correction should take into account "the nature of the personal information and the purposes of the processing of the personal information." The right should have limited application to personal information that is necessary for the consumer to receive services (e.g. name, contact and payment information) and to exercise rights related to the business (e.g. payment or credit history with the business). It should not apply to data points that are obtained from third parties or are generated automatically through use of the business' services and that do not impact the consumer's rights or services (e.g. IP address, inferences, or telemetry data). It should not apply to inferences made about the consumer or to information obtained from third parties, unless this information is necessary to provide services to the consumer.

A consumer should not be permitted to alter a contract or terms to which s/he has agreed by exercising the right to correction.

Regulations should have provisions on verification of identity similar to those of the CCPA (11 C.C.R. §999.323-999.326). Businesses should be able to develop processes to prevent fraud, such as using the precise geolocation of a consumer to verify identity, or the staggering of timeframes in which certain data is corrected. It is essential for businesses to be

able to use strong methods of authenticating consumers' identities prior to releasing or changing personal information.

Separately, when consumers request a correction to personal information, they must be required to show that the requested change is necessary and accurate by showing proof like a phone bill.

A business that receives a consumer's request to correct information should not be required to correct information if it was not the original source of the information. For example, a business may have information in its system that was inputted incorrectly by the consumers themselves and shared by another party. A business that was not the original source of the information should be able to inform the consumer to contact the original source so that the information is corrected at its source. Otherwise, incorrect data will continue to feed back into business systems.

Right to Know

A business should be required to provide information in response to a consumer request to know if it is readily available and in electronic format. To contrast, a business that has information in archive systems or non-electronic formats should be able to claim that providing such information "would involve a disproportionate effort."

5) 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.

Data is vital for preventing incidents like fraud and securing network. Personal information was instrumental in promoting public safety like stopping the San Bernardino shooters, expanding consumer access to credit, and improving public health.² An interpretation of the CPRA by the Agency should take into consideration these societally beneficial purposes when determining when opt-out is not required.

Private and public implementations of universal opt-outs can have negative spillover effects for both individual companies and the broader internet ecosystem. Because of this, the design of these mechanisms should be developed collaboratively with input from industry and other stakeholders. Regulations must be consistent with the text of the CPRA, which clarifies that it is optional for a business to recognize a signal to opt out of the sale or sharing of personal information or to limit the use of sensitive information (§1798.135(b)(1), (3)). Other consumer notice and competition considerations contained in §1798.185(a)(19)(A) must also be reflected in the rules. Moreover, the CPRA directs the CPPA to cooperate with other states to ensure consistent application of privacy protections. § 1798.199.40(i). Colorado also is poised to start a rulemaking on an opt-out signal with regulatory directives to consider similar, and in some instances nearly identical, specifications to what the CPRA directs. The CPPA should work with Colorado to ensure that interoperable and aligned requirements for these signals are developed.

² https://americaninnovators.com/wp-content/uploads/2020/10/CTEC_TechUpgrade_Data_.pdf

Any specifications that apply to global privacy controls (“GPC”) should provide businesses with sufficient flexibility to implement the technical solutions that fit their business models. Businesses use a variety of solutions today, and the Agency should avoid mandating a specific type of solution that may thwart innovation and reduce incentives to provide consumers the full range of choices in opt-out solutions. Any specifications must accurately identify which consumers are located in California so that businesses can accurately honor the request. Businesses should be limited to online data collection and not require a company to identify unauthenticated users to ensure that they are opted out of all forms of “sale” of personal information. This would be inconsistent with §1798.145(j). Businesses must be able to notify consumers of the consequences of an opt-out and solicit permission to use cookies. This is consistent with the CPRA’s aims of transparency and consumer choice. Any GPC must inform users of the meaning of the “Do Not Sell” signal in California. Default choices must be avoided to prevent uninformed choice or market distortion.

Companies honoring opt-out signals will inevitably receive competing signals (i.e. - a person opts out through a universal control but then opts in for a specific service). It will be important to provide guidance to companies about how to manage competing signals.

Ample time is needed by companies to adhere to any preference signal not obtained directly. If the signal is an incoming global request from a browser, another platform, etc, businesses need IT resources to read and direct traffic into our direct request/response system. Time would be necessary to adjust based on the preference signal that may be developed. In the interim, the preference signal solution should direct consumers to the individual companies to handle their specific requests, so consumer needs are met.

Companies should have the ability to win back people on an individual basis. There should be guardrails for this, but the relationship that businesses build with their customers should be preserved. For instance, a company could give users the ability to win back opportunities for some extended period of time.

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

Businesses should only be able to provide identifiable personal information that is readily and reasonably available in their active production systems and does not present undue administrative cost or burden. The Agency should consider that this information may be harmful if exposed and is actively in use. Consumers should be allotted one request per 12 months for requests for data.

Businesses could spend disproportionate efforts to provide personal information from unstructured environments (e.g. log files), archived, non-active or non-production systems, and personal information that may not be identifiable on its own. The regulations should establish that IP addresses are not considered personal information if a business does not link the IP address with a specific person. For example, if an IP address is considered personal information, it is not individually identifiable on its own. The business may have to tie multiple pieces of

data, systems, and vendor/partner data together to attempt to properly identify the individual, which could increase privacy risks for consumers. If identifiable information could even be provided back, the information is not digestible by the average consumer. CCPA does not require the business to reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personally identifiable information (e.g. aggregated, pseudonymized, or deidentified data).

8) Definitions and Categories

The CCPA and CPRA provide for various regulations to create or update definitions of important terms and categories of information or activities covered by the statute.

c. Updates, if any, to the law’s definitions of “deidentified” and/or “unique identifier.”

The Agency should align the definition of “deidentified” with the Virginia Consumer Data Privacy Act’s (“VCDPA”) definition for clarity and better implementation. The Agency should remove the reference to inferring information, add a reference to devices linked to a consumer, and sharpen the distinction between “pseudonymized” and “deidentified” data by applying exceptions similar to those in the VCDPA and Colorado Privacy Act (“CPA”). There should also be the added benefit of incentivizing the use of privacy protective technologies even where deidentification may not be feasible.

In the definition of “unique identifier,” the Agency should remove references to devices linked to a consumer and the list of example identifiers. Doing so would clarify the definition, remove circular references, and align the treatment of linked devices with VCDPA. “Unique identifier” shouldn’t include cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; that is information that might link to a unique identifier. The technology or cookies themselves wouldn’t be uniquely identifying the individual. It would be helpful to clarify that the identifier is unique if the persistent identifier can *reasonably* identify the individual without the burden on the business to reidentify and link other data to make it individually identifiable.

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

The current list of business purposes includes auditing, ensuring security and integrity, debugging, short-term transient use including non-personalized advertising shown as part of a current interaction, performing services on behalf of the business including maintaining or servicing accounts, providing advertising and marketing services except for cross-context behavioral advertising, undertaking internal research, and undertaking activities to verify or maintain the quality or service of a service or device.

Businesses rely on these established permissible uses to help improve their products, detect and prevent fraud, protect the security of the information of their customers, and generally support their services. With that in mind, it is important to preserve the current list.

h. What definition of “specific pieces of information obtained from the consumer” the Agency should adopt.

The regulations should clarify that “specific pieces of information” should not include data stored client-side/on user-device only, and non-human readable data. Platforms will not have access to the former, and the latter will typically be of little practical use for individuals.

i. The changes, if any, that should be made to further define “precise geolocation.”

Industry technical standards for precision utilize decimal points of latitudinal and longitudinal coordinates rather than a radius. It would be helpful to clarify the definition of “precise geolocation” to align to industry technical standards. At minimum, the regulations should explain how a radius of 1,850 feet translates into latitude/longitude coordinates.

j. The regulations, if any, that should be adopted to further define “dark patterns.”

Regulations should avoid setting technical specifications or image requirements that constitute “dark patterns.” Any regulations in this area should also be consistent with any guidance or reports issued by the Federal Trade Commission, which is also investigating this subject. It should align with the rich body of FTC case law, which turns on whether the misrepresentation or omission is material.

The definition of “dark pattern” in the CPRA would be impossible for companies to implement. Rather than describing the elements of a dark pattern, it focuses on the *effect* of the interface- specifically whether it subverts or impairs people’s autonomy, decision-making, or choice. The current definition would have the unintentional consequence of prohibiting privacy-protective default settings because they would impair choice and autonomy (e.g. - where location sharing is automatically toggled off and the consumer has to toggle it back on to share location data).

The use of an examples-based approach is particularly important because this is a novel area of regulation. It will be important to recognize that companies do not have existing familiarity with design-related requirements. Therefore, it will be critical to provide significant guidance. In particular, the Chamber requests that the Agency more specifically defines the practices that constitute dark patterns. For example, this could include practices like displaying one option prominently while making it hard to see or access another option. In short, the goal should be to eliminate bad practices by providing clear guidance to companies about what those practices are. Instead, the current text would have companies attempt to understand whether the design of their website or app impacts a person’s “autonomy” -- a vague, if not impossible to meet, standard.

Regulations should balance clear and precise descriptions of risky practices with the risk of negative effects from overly prescriptive design. The best design is context sensitive, consistent with the wider user experience and a users' expectations. It should be aware of the particular goals and intent that a person may have at that time in the user journey.

Again, because this is a novel area of regulation, it will be important to continue to consult with a range of stakeholders, but particularly with designers, to understand design constraints and design best practices.

The Chamber appreciates the ability to provide comments on the issue areas requested above. Another area in which the Agency should consider harmonizing approaches with other states is enforcement. Virginia and Colorado provide at least a 30-day cure period for alleged violations before enforcement is undertaken. The CPRA gives the Agency discretion to provide businesses with a cure period.³ The Chamber requests that the Agency promulgate a blanket 30-day cure period to enable greater collaboration between businesses and regulators.

We look forward to working with you to ensure consumer protection and clear rules for compliance in implementing the CPRA.

Sincerely,



Jordan Crenshaw
Vice President
Chamber Technology Engagement Center

³ Cal. Civ. Code § 1798.199.45 (Upon the sworn complaint of any person or on Its own initiative, the Agency may investigate possible violations of this title relating to any business, service provider, contractor, or person. **The Agency may decide** not to Investigate a complaint or decide **to provide a business with a time-period to cure the alleged violation. In making a decision not to investigate or provide more time to cure, the Agency may consider: (a) the lack of Intent to violate this title; and (b) voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the Agency of the complaint.** The Agency shall notify in writing the person who made the complaint of the action, If any, the Agency has taken or plans to take on the complaint, together with the reasons for such action or non-action.)

From: Christopher Oswald [REDACTED]
Sent: 11/8/2021 11:38:47 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 Ad Trade Response to CPPA Invitation for Preliminary Comments on Proposed CPRA Rulemaking
Attachments: FINAL Joint Ad Trade Comments - CPRA Preliminary Rulemaking Request for Comment.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

To: regulations@cppa.ca.gov

Subject: PRO 01-21 Ad Trade Response to CPPA Invitation for Preliminary Comments on Proposed CPRA Rulemaking

To Whom It May Concern:

Please find attached comments from the following advertising trade associations in response to the California Privacy Protection Agency's request for preliminary comments on proposed rulemaking under the California Privacy Rights Act: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the Network Advertising Initiative, the American Advertising Federation, and the Digital Advertising Alliance. We appreciate your consideration of these comments.

If you have any questions about these comments, please feel free contact me.

Regards,

Christopher Oswald

Senior Vice President, Government Relations

ANA – Association of National Advertisers

[REDACTED] | ana.net | [@ANAGovRel](https://twitter.com/ANAGovRel)

2020 K Street, NW, Suite 660, Washington, DC 20006



November 8, 2021

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

RE: Joint Ad Trade Comments 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)

Dear California Privacy Protection Agency:

On behalf of the advertising industry, we provide the following initial, but not exhaustive, comments in response to the California Privacy Protection Agency ("Agency") invitation for preliminary comments on the proposed rulemaking under the California Privacy Rights Act of 2020 ("CPRA").¹ We look forward to offering ongoing input to the Agency to help develop effective and workable regulations implementing the CPRA. We believe the implementing regulations can be drafted in a way that provides robust consumer protections while still allowing Californians to enjoy the full benefits of the data economy. Implementing rules, provided in a timely manner, are vital to ensuring consumers have access to the rights provided under the CPRA while also helping businesses operationalize the law's numerous new requirements.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses, to household brands, advertising agencies, and technology providers, including a significant number of California businesses. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend. Digital advertising contributes more than 1.1 million jobs to the California economy and approximately \$2.4 trillion to the United States' gross domestic product ("GDP").² Our members engage in responsible data collection and use that benefits consumers and the economy, and we believe consumer privacy deserves meaningful and effective protections in the marketplace.

Our organizations responded to every request for comment from the California Attorney General ("OAG") to further its efforts to promulgate regulations under the California Consumer Privacy Act of 2018 ("CCPA"). For your reference, our comments in response to those requests are attached hereto as **Exhibit A**. We have consistently supported providing Californians with appropriate notice of businesses' data practices as well as the ability for those California consumers to exercise effective choices related to those practices. We ask the Agency to take our past

¹ See California Privacy Protection Agency, *Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020*, located [here](#) (hereinafter, "RFC").

² See John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 5, 121-23 (Oct. 18, 2021), located [here](#).

comments on the CCPA regulations into account as it begins the process of drafting regulations to implement the CPRA. We also ask the Agency to consider the following specific topics when issuing its initial draft regulations:

- I. The Agency Should Take a Leadership Role in Aligning State Privacy Laws.** The Agency is in a unique position to advance harmonization across differing state privacy laws, such as those in Virginia and Colorado. To the extent possible, we encourage the Agency to take steps to further uniformity across state privacy regimes.
- II. The Agency Should Ensure Opt-Out Preference Signals Are Truly User-Enabled and Are Not Set By Default.** The Agency should promulgate rules that reinforce the CPRA's requirement for opt-out preference signals to be affirmatively set by consumers. The Agency should prohibit intermediaries from setting such signals by default and should ensure that opt-out signals or other mechanisms do not inhibit businesses from communicating the consequences of opt out choices to consumers. We believe that this is in conformance with the California privacy laws.
- III. The Agency Should Appropriately Tailor Risk Assessment Requirements.** The Agency should require businesses to submit assessments only upon request in the context of a formal investigatory proceeding. The Agency should also make clear that turning assessments over to the Agency does not waive bedrock attorney-client privilege and work product protections.
- IV. The Agency Should Avoid Overly Prescriptive Rules Addressing Dark Patterns.** The Agency's dark patterns regulations should not overly constrain businesses' ability to engage with consumers. Such regulations should strike a balance of deterring deceptive and manipulative conduct while allowing for flexibility in the modes, methods, and content of business communications with consumers.
- V. The Agency Should Take Steps to Preserve the Benefits That Data-Driven Advertising Provides to Californians, to the Economy, and to All Consumers.** The Agency should recognize the benefits the data driven economy provides to consumers and should advance a regulatory approach that offers appropriate protections for Californians while still enabling them to benefit from the data economy.

We thank the Agency for the opportunity to provide comment on these topics, as discussed in more detail below, and we look forward to continuing to engage with the Agency as it promulgates draft regulations to implement the CPRA.

I. The Agency Should Take a Leadership Role in Aligning State Laws

In addition to California, Virginia and Colorado have recently enacted state privacy laws that are set to take effect in 2023.³ To the extent possible, we encourage the Agency to use the

³ Va. Code Ann. §§ 59.1-571 et seq.; Colo. Rev. Stat. §§ 6-1-1301 et seq.

regulatory process to work to harmonize the CPRA's requirements with privacy law requirements in other states. Although California was the first mover in the state privacy space and the Agency has been tasked with issuing regulations to address specific issue areas within the CPRA, the Agency should work to ensure its regulations' terminology and definitions align with other state laws to the extent practicable. Such alignment is in the best interest of consumers, the nation's policy on data privacy, and businesses alike. Because California is the first state to adopt broad data privacy regulations, the Agency has the unique opportunity to show leadership in this space by advancing harmonization of potentially conflicting state law standards.

Advancing uniformity across state privacy law requirements would not only create a more streamlined and less costly compliance environment for businesses with a national footprint,⁴ but it would also minimize consumer confusion about potentially varying privacy rights and protections afforded in different states. In the absence of a national data privacy standard set by Congress, we ask the Agency to work intentionally to ensure its CPRA regulations are unified with, or at the very least do not conflict with, data privacy laws in other US jurisdictions.

II. Ensure Opt-Out Preference Signals Are Truly User-Enabled and Are Not Set By Default

In the Agency's invitation for preliminary comments, it requested comment on "[h]ow businesses should process consumer rights that are expressed through opt-out preference signals."⁵ The CPRA appropriately sets a standard that enables businesses to elect whether to offer consumers the ability to opt out through a homepage link or through an opt out preference signal mechanism sent with the consumer's consent. We encourage the Agency to follow the explicit directives set forth in the CPRA by ensuring its rules surrounding opt-out preference signals further true consumer choice, allow businesses to communicate the consequences of opt out decisions to Californians, and do not allow opt-out preference signals to be set by intermediaries by default.

A. Legal Standard

The CPRA sets out a specific standard dictating when businesses must honor opt-out preference signals. According to the CPRA, businesses "**may elect**" to either "(a)... [p]rovide a clear and conspicuous link on the business's internet homepage(s) titled 'Do Not Sell or Share My Personal Information'" **or** (b) allow consumers to "opt-out of the sale or sharing of their personal information... through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]"⁶ The CPRA makes this business choice explicitly clear by stating: "**A business that complies with subdivision (a) of this Section is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or (b).**"⁷ The CPRA therefore sets forth clear rules that specifically state businesses can elect whether or not to offer

⁴ Estimated initial costs for CCPA compliance stand at a staggering \$55 billion dollars, and estimated initial compliance costs for other state proposals, such as those in Florida, range from \$6.2 billion to \$21 billion. See California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* at 11 (Aug. 2019), located [here](#); see also Florida Tax Watch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida* at 2 (Oct. 2021), located [here](#).

⁵ RFC at 5.

⁶ CPRA, Cal. Civ. Code §§ 1798.135(a), (b) (emphasis added).

⁷ *Id.* at § 1798.135(b)(3) (emphasis added).

consumers an opt-out preference signal option or an option to opt out via a clearly labeled homepage link.

B. Opt-Out Preference Signals Should Be User-Enabled

For businesses that elect to enable consumers to opt out of sales or sharing of personal information through opt-out preference signals or other such mechanisms, the CPRA directs the Agency to promulgate rules defining technical specifications for such controls. The CPRA places specific parameters around the Agency’s promulgation of such rules. Namely, the opt-out signal or mechanism must “ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal **cannot unfairly disadvantage another business.**”⁸ According to the CPRA, the Agency must also ensure such opt-out preference signals or controls “clearly represent a consumer’s intent and [are] **free of defaults constraining or presupposing such intent.**”⁹ The regulations should reflect these important elements of consumer choice that are set forth in the law. These parameters serve to help ensure consumer choices are genuine, and that opt-out preference signal regulations do not favor certain businesses over others, remove businesses’ ability to communicate the consequences of opt out choices to consumers, or stand in the way of true and informed user choice.

Our past comments to the CCPA detail this issue in depth, as set forth in **Exhibit A**. In particular, beginning on page 2 of our March 27, 2020 comment to the OAG on the content of the CCPA regulations, we discussed ways that intermediary interference with consumers’ use of global privacy controls could thwart the expression of true user choices. Finally, we addressed how the imposition of a global privacy control requirement should not turn the CCPA’s and CPRA’s explicit opt-out structure into an opt-in structure, thereby directly contravening the text of the law itself, which enables consumers to opt out of business sales of personal information, rather than have to turn off an automatic setting that assumes they want to opt out of sales across all businesses. We ask the Agency to review these comments for background and to ensure that regulations implementing the CPRA further informed consumer choice and the explicit opt out structure set forth in the law.

In addition, we provide in **Exhibit B** a consensus framework for evaluating whether opt-out preference signals or other mechanisms in the market are actually *user-enabled*. This consensus framework was developed by a broad group of stakeholders across the digital advertising industry. It requires an affirmative consumer choice to exercise the right to opt out and requires choice settings to be presented to consumers in ways that do not unfairly disadvantage certain businesses over others. The framework also requires a business to communicate the effect of the choice setting and the scope of the opt out to consumers. The framework also provides guidance regarding business transparency surrounding the choice signal and how consumers can opt in after previously having opted out of sales or sharing. We encourage the Agency to review the framework set forth in **Exhibit B** and to consider implementing it via regulation.

⁸ *Id.* at § 1798.185(19)(A)(i) (emphasis added).

⁹ *Id.* at § 1798.185(19)(A)(iii) (emphasis added).

C. Jurisdictional Signals

To ensure user choice is given the full force and effect under law, the Agency should permit a business to authenticate individuals submitting opt out requests as residents of California. Californians' rights to opt out of personal information sales and sharing may differ from the rights afforded to consumers in other states come 2023. For instance, in Virginia and Colorado, consumers will have the ability to opt out of "sales," "targeted advertising," and "profiling," as defined by those states' respective privacy laws. So that a business can determine the applicable state law and apply it accordingly, it is vital that requests indicate the relevant jurisdiction. The Agency should therefore take steps to clarify that opt-out preference signals must come with a jurisdictional tag so that businesses can afford the rights and privileges to consumers that align with their state of residence.

D. Default Settings

Californians should be permitted to exercise control over personal information associated with them, and that right should not be usurped by intermediary companies who stand between consumers and their access to the Internet. We ask the Agency to take steps to ensure that any technical standard or regulation promulgated surrounding opt-out preference signals or other global controls requires such mechanisms to be truly user-enabled and not set by default. Opt-out mechanisms should not permit such decisions to be set by intermediary companies or to be turned on by default. Ensuring that consumers – and not platforms, browsers, or other intermediaries – can make informed choices about personal information relating to them will help to ensure consumer preferences are carried out and consumer expectations are met.

We also encourage the Agency to issue regulations to make sure that opt out preference signals or other similar mechanisms are accompanied by effective notices that appropriately explain the effects and scope of choices that are available to consumers. Consumers should be given information about the consequences of their opt out choices so they can make informed privacy decisions. However, certain global privacy control implementations already in the marketplace are unconfigurable and set by default.¹⁰ These default, unconfigurable controls inhibit consumers' ability to receive information about the implications of their privacy decisions. For example, the disclosures associated with the Brave browser's "Global Privacy Control" plugin provide no information on how the global control will impact the consumer, such as by increasing the likelihood the consumer will encounter paywalls or decreasing consumer's ability to receive ads that are personalized or relevant to them.¹¹ Global controls like this directly conflict with the requirements of CPRA, which require such controls to be free from defaults and "clearly described."¹² The Agency should take steps to ensure its regulations require opt out preference signals to be user-enabled and allow the effects of such signals to be appropriately explained to consumers.

¹⁰ See Brave, *Global Privacy Control, a new Privacy Standard Proposal*, now Available in Brave's Desktop and Android Testing Versions, available at <https://brave.com/web-standards-at-brave/4-global-privacy-control/> ("Importantly, Brave does not require users to change anything to start using the GPC to assert your privacy rights. For versions of Brave that have GPC implemented, the feature is on by default and unconfigurable.")

¹¹ *Id.*

¹² CPRA, Cal. Civ. Code § 1798.185(19)(A)(iii).

III. Appropriately Tailor Risk Assessment Requirements

The Agency asked commenters to provide input on when processing should require a risk assessment under CPRA.¹³ We encourage the Agency to: (1) require businesses to submit assessments to it only upon the Agency's request pursuant to a civil investigative demand or other formal investigatory process; (2) clarify that a single assessment conducted for purposes of compliance with other laws may satisfy CPRA assessment requirements; and (3) ensure that any requirements to turn over assessments to the Agency do not waive foundational attorney-client privilege or work product protections.

We ask the Agency to clarify that risk assessments must be provided to the Agency only upon request after it has served a civil investigative demand or similar formal inquiry on a business. Requiring risk assessments at any more regular cadence would create excessive compliance costs for businesses and would necessitate significant resources from the Agency to review assessments, thereby removing staff from devoting time to other areas of critical importance. In this area, the Agency can take steps to align the CPRA with other state privacy laws. For example, the Virginia Consumer Data Protection Act allows the Virginia Attorney General to request a company's data protection assessment pursuant to a civil investigative demand if such assessment is relevant to an ongoing investigation.¹⁴ The Agency should adopt a similar approach to risk assessments under CPRA.

The Agency should also clarify that assessments conducted for purposes of compliance with other laws may satisfy CPRA requirements if the assessment conducted for compliance with another law addresses a comparable set of processing operations or includes similar activities. Laws that will go into effect imminently, such as the new privacy laws in Colorado and Virginia, require assessments for certain processing activities. Companies should not be required to perform separate assessments for each law if the processing activity that is the subject of the assessment is similar. The Agency should confirm that assessments conducted to comply with other privacy laws may satisfy CPRA requirements.

Finally, we encourage the Agency to clarify that a disclosure of a risk assessment to the Agency upon its request does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment. Attorney-client privilege and work product protections are crucial, long-standing principles that encourage open communications between businesses and their counsel. Declining to clarify that such protections extend to risk assessments would hinder businesses from being able to candidly work with their legal representatives to perform risk assessments to further compliance with data privacy laws. As a result, the Agency should clarify that its risk assessment regulations and any actions that would require a business to turn over risk assessments to the Agency do not waive critical attorney-client or work product protections.

¹³ See RFC at 2.

¹⁴ Va. Code. Ann § 59.1-576(c).

IV. Avoid Overly Prescriptive Rules Addressing Dark Patterns

In its request for comment, the Agency asked for input on “regulations, if any, that should be adopted to further define ‘dark patterns.’”¹⁵ The CPRA itself defines “dark pattern” to mean “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.”¹⁶ If the Agency takes steps to promulgate further regulations surrounding dark patterns, we ask it to avoid overly prescriptive mandates that do not enable flexibility for business communications with consumers.

While we agree the Agency should take steps to prevent unscrupulous actors from using deceptive and manipulative practices in the marketplace, we strongly believe overly prescriptive rules regulating the form and content of speech would not be in the best interests of California consumers or businesses. Notices and choice interfaces that are presented to consumers should be clear, meaningful, and free from deceptive practices that manipulate consumers into making certain elections. However, there should be flexibility for companies, channels, and platforms to present user information, choices, and notices to consumers in ways that make sense for the given company, channel, platform, and the consumer. For instance, a brick and mortar retailer may present notices and choices to consumers in a manner that is entirely different from a company that offers a smart speaker with no visible interface for written disclosures on the device. Regulations addressing dark patterns should not be so rigid that they limit businesses’ ability to appropriately tailor and present disclosures and choices to their consumers, nor should they require businesses to present information in a way that lessens consumer engagement or hinders business innovation. We caution the Agency from overreaching in its rules on dark patterns, as overly prescriptive regulations could violate First Amendment protections for commercial speech as applied to the states through the due process clause of the Fourteenth Amendment.¹⁷

Responsible businesses do not endeavor to be deceptive or manipulative in their communications with consumers, because their relationships with customers are founded in consumer trust. Businesses are incentivized to maintain that relationship of trust with customers so consumers continue to come to them for products and services. We support regulations that would minimize deceptive and manipulative market practices when it comes to presenting consumer notices and choice interfaces, as we believe truthful, accessible, and clear notices and choice mechanisms benefit businesses and consumers alike. However, we ask the Agency to avoid issuing overly prescriptive rules that would too rigidly define how businesses must communicate with and present choices to consumers.

V. Data-Driven Advertising Provides Significant Benefits to Californians, to the Economy, and to All Consumers

Over the past twenty years, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A new study found that the Internet economy’s contribution to the United States’ GDP grew 22 percent per year since 2016 in a national economy that grows

¹⁵ RFC at 6.

¹⁶ CPRA, Cal. Civ. Code § 1798.140(l).

¹⁷ See Exhibit A, December 27, 2020 Ad Trade Comments on Fourth Set of Proposed Modifications to Text of Proposed California Consumer Privacy Act Regulations at 3-6.

between two to three percent per year.¹⁸ In 2020 alone, the Internet economy contributed \$2.45 trillion to the U.S.'s \$21.18 trillion GDP, which marks an eightfold growth from the Internet's contribution to GDP in 2008 of \$300 billion.¹⁹ Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet, which amounts to 7 million more jobs than four years ago.²⁰ More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated 34 percent.²¹ The same study found that the ad-supported Internet contributed 1,111,460 full-time jobs across the state of California, well more than double the number of Internet-driven jobs from 2016.²²

A. Advertising Fuels Economic Growth

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive regulation that significantly hinders certain advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy.²³ One recent study found that “if third-party tracking were to end “without mitigation” [t]he U.S. open web’s independent publishers and companies, who are reliant on open web tech, would lose between \$32 and \$39 billion in annual revenue by 2025.”²⁴ That same study found that the lost revenue would become absorbed by “walled gardens,” entrenched market players, thereby consolidating power and revenue in a small group of powerful entities.²⁵ Smaller news and information publishers, multi-genre content publishers, and specialized research and user-generated content would lose more than an estimated 15.5 billion in revenue.²⁶ Data-driven advertising has thus helped to democratize economic market power, ensuring that smaller online publishers can remain competitive with large corporations. A recent study showed that “long tail” publishers rely on third-party advertising technology, which accounts for approximately two-thirds of their advertising activity.²⁷

B. Advertising Supports Californians’ Access to Online Services and Content

In addition to providing economic benefits, data-driven advertising subsidizes the vast and varied free and low-cost content publishers offer consumers through the Internet, including public health announcements, news, and life-saving information about COVID-19, in addition to other critical public health information related to missing children and catastrophic weather events such

¹⁸ See John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 5 (Oct. 18, 2021), located [here](#).

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.* at 6.

²² Compare John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 121-23 (Oct. 18, 2021), located [here](#) with John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem*, INTERACTIVE ADVERTISING BUREAU, 106 (2017), located [here](#) (finding that Internet employment contributed 478,157 full-time jobs to the California workforce in 2016 and 1,111,460 jobs in 2020).

²³ See John Deighton, *The Socioeconomic Impact of Internet Tracking* 4 (Feb. 2020), located at <https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf>.

²⁴ *Id.* at 34.

²⁵ *Id.* at 15-16.

²⁶ *Id.* at 28.

²⁷ Digital Advertising Alliance, *Study: Online Ad Value Spikes When Data Is Used to Boost Relevance* (Feb. 10, 2014), located at <https://digitaladvertisingalliance.org/press-release/study-online-ad-value-spikes-when-data-used-boost-relevance>.

as wildfires.²⁸ Advertising revenue is an important source of funds for digital publishers,²⁹ and decreased advertising spends directly translate into lost profits for those outlets. Since the coronavirus pandemic began, 62 percent of advertising sellers have seen advertising rates decline.³⁰ Publishers have been impacted 14 percent more by such reductions than others in the industry.³¹ Revenues from online advertising support the cost of content that publishers provide and consumers value and expect. Regulations that inhibit or restrict preferred methods of digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, thereby compounding the detrimental impacts to the economy presented by COVID-19. The effects of such legislative models ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

C. Consumers Prefer Personalized Ads

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. One study found more than half of consumers (53 percent) desire relevant ads, and a significant majority (86 percent) desire tailored discounts for online products and services.³² Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.³³ Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.³⁴

The ability of consumers to provide, and of companies to responsibly collect and use, consumer data has been an integral part of the dissemination of information and the fabric of our economy for decades. The collection and use of data are vital to our daily lives, as much of the content we consume over the Internet is powered by open flows of information that are supported by advertising. We therefore respectfully ask you to carefully consider the potential impact of any

²⁸ Digital Advertising Alliance *Summit Snapshot: Data 4 Good – The Ad Council, Federation for Internet Alerts Deploy Data for Vital Public Safety Initiatives* (Sept. 2, 2021), located at <https://digitaladvertisingalliance.org/blog/summit-snapshot-data-4-good-%E2%80%93-ad-council-federation-internet-alerts-deploy-data-vital-public>.

²⁹ See Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

³⁰ IAB, *Covid's Impact on Ad Pricing* (May 28, 2020), located at https://www.iab.com/wp-content/uploads/2020/05/IAB_Sell-Side_Ad_Revenue_2_CPMs_5.28.2020.pdf

³¹ *Id.*

³² Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located at https://www.thompsoncoburn.com/docs/default-source/Blog-documents/consumer-attitudes-toward-relevant-online-behavioral-advertising-crucial-evidence-in-the-data-privacy-debates.pdf?sfvrsn=86d44cea_0.

³³ Digital Advertising Alliance, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf.

³⁴ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

new regulations on data-driven advertising, the consumers who reap the benefits of such advertising, and the overall economy before advancing them through the rulemaking process.

* * *

In addition to the specific issues set forth above, we encourage the Agency to continue to engage with stakeholders who are impacted by the CPRA as it begins the process of drafting implementing regulations. Clear and consistent communication between consumers, businesses, the Agency Board, staff, and others involved in the CPRA regulatory process will be crucial to develop regulatory provisions that further the goal of advancing consumer privacy. We welcome future opportunities to respond directly to the regulatory provisions the Agency drafts. We hope to have a meaningful two-way dialogue on these important topics.

Thank you for your consideration of these comments. We look forward to working further with you on developing implementing regulations under CPRA.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
202-269-2359

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
202-269-2359

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
202-800-0771

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

EXHIBIT A



December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Dear Attorney General Becerra:

As the nation's leading advertising and marketing trade associations, we provide the following comments to offer input on the California Office of the Attorney General's ("OAG") proposed regulations implementing the California Consumer Privacy Act ("CCPA"). We and our members support the objectives of the CCPA and believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, we have certain concerns about negative consequences the proposed regulations could create for consumers and businesses alike. Additionally, we are concerned that many of the proposed rules' provisions impose entirely new requirements on businesses that are outside of the scope of the CCPA and do not further the purposes of the law.

The undersigned organizations collectively represent thousands of companies in California and across the country, from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of the U.S. advertising spend and drives more than 80 percent of our nation's digital advertising spend. Locally, our members help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.¹ The companies we represent desire to comply with the CCPA by offering consumers robust privacy protections while simultaneously continuing to be able to do business in ways that benefit California's employment rate and its economy.

We provide the following comments to draw the OAG's attention to certain parts of the proposed regulations that are unsupported by statutory authority and other provisions that may have detrimental consequences for consumers and businesses alike. Below we provide a list of suggested updates to the proposed rules to bring them into conformity with the text of the CCPA and to rectify certain negative results they could cause for consumers and businesses. We also highlight certain provisions in the proposed regulations that we support for providing helpful clarity to the advertising and marketing industry. Some of the undersigned trades will file additional comments to the OAG.

¹ IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <https://www.ana.net/magazines/show/id/rr-2015-ihs-ad-tax>.



I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.² Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.³

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the FTC noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁴ It is in this spirit—preserving the ad supported digital and offline media marketplace while helping to design privacy safeguards—that we provide these comments.

² John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017) <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

³ *Id.*

⁴ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.



II. The OAG Should Ensure the Proposed Regulations' Definitions Conform with the Text of the CCPA and Are Given Consistent Meaning

Although the OAG has provided definitions for several new terms in the proposed regulations, some of the definitions contradict the text of the CCPA itself and others are used inconsistently throughout the proposed regulations, thereby obscuring the meaning of the defined terms. For example, the OAG defined “request to know” in a way that departs from the text of the CCPA. In addition, the use of the defined term “request to delete” in at least one section of the proposed regulations is at odds with its definition in the proposed regulations as well as the text of the CCPA. We respectfully ask the OAG to update the proposed regulations so that the defined terms conform with the text of the CCPA and are given consistent meaning throughout the entirety of the draft rules.

The OAG defined “request to know” as “a consumer request that a business disclose personal information that it has about the consumer... [including] [s]pecific pieces of personal information that a business has about a consumer....”⁵ This definition differs from the text of the CCPA, which states that “[a] consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer...” the categories and specific pieces of personal information “it has *collected about the consumer*.”⁶ To reduce business and consumer confusion and align the proposed regulations with California legislators’ intent and the text of the CCPA, the OAG should update the proposed rules so a “request to know” is defined as “a consumer request that a business disclose personal information that it has collected about the consumer... [including] [s]pecific pieces of personal information that a business has collected about a consumer.”

In addition, the OAG defined “request to delete” as “a consumer request that a business delete personal information about the consumer that the business has collected from the consumer....”⁷ This definition aligns with the deletion right as it is set forth in the CCPA, which states that “[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”⁸ However, in the section of the proposed regulations discussing the information that must be included in a privacy policy, the draft regulations note that a business must “[e]xplain that a consumer has a right to request the deletion of their personal information *collected or maintained* by the business.”⁹ The expression of the right to delete in the privacy policy section of the proposed regulations therefore contradicts with the CCPA’s stated expression of the right and the proposed regulations’ defined term “request to delete.” The OAG should update the privacy policy section of the CCPA so it states that a business must explain that consumers have the right

⁵ Cal. Code Regs. tit. 11, § 999.301(n)(1) (proposed Oct. 11, 2019).

⁶ Cal. Civ. Code §§ 1798.110(a)(1), (5) (emphasis added).

⁷ Cal. Code Regs. tit. 11, § 999.301(o) (proposed Oct. 11, 2019).

⁸ Cal. Civ. Code §§ 1798.105(a).

⁹ Cal. Code Regs. tit. 11, § 999.308(b)(2)(a) (proposed Oct. 11, 2019) (emphasis added).



“to request personal information about the consumer that the business has collected from the consumer” to align the section with the defined term “request to delete” and the CCPA.

As described above, we suggest that the OAG take steps to alter certain definitions in the proposed regulations so that they match and support the text of the CCPA and are used consistently throughout the draft rules. Such updates would help create certainty for businesses and consumers and would ensure that the text of the CCPA and the proposed regulations interpreting its terms are not in conflict.

III. Allow Flexibility for Businesses that Do Not Collect Information Directly to Provide Notice of Sale and an Opportunity to Opt Out

The CCPA states that a “third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out....”¹⁰ Through the proposed regulations, the OAG has provided that the business must: (1) contact the consumer directly to provide notice of sale and notice of the right to opt out, or (2) confirm the source provided a notice at collection to the consumer; obtain signed attestations from the source describing how it gave notice at collection, including an example of the notice given to the consumer; retain such attestations and sample notices for two years; and make them available to consumers upon request.¹¹ The OAG should change this provision of the draft rules so businesses are not required to maintain and make available examples of the notice provided to a consumer at the time of collection.

Requiring businesses to maintain sample notices creates a substantial new business obligation that was not contemplated by the legislature when it passed or amended the law. Requiring examples of the notice that was provided to a consumer at the time of collection constitutes a requirement that is beyond the text, scope, and intent of the CCPA, as the law itself only requires a third party to ensure a consumer has received explicit notice of sale and an opportunity to opt out. Second, little if any additional consumer benefit is provided through this new business duty to maintain example notices. The requirement to obtain attestations from data sources confirming that a notice at collection was given and describing how the notice was given provides consumers with the same transparency benefits as requiring businesses to obtain and maintain samples of the notice that was given to consumers.

Finally, mandating that businesses must maintain examples of notices provided to consumers at the time of collection is unreasonable, significantly burdensome, and could place a considerable strain on normal business operations. For example, it is possible the proposed regulations could be interpreted to require businesses to pass example notices from original sources of data to third party businesses who may later receive personal information. This obligation would impose significant new recordkeeping obligations on third party businesses and could stifle the free flow of information that powers the Internet. We therefore ask the OAG to

¹⁰ Cal. Civ. Code § 1798.115(d).

¹¹ Cal. Code Regs. tit. 11, § 999.305(d) (proposed Oct. 11, 2019).



remove the requirement for businesses to obtain examples of the notices at collection that were given to consumers to enable more flexibility for businesses to comply with the requirements the CCPA places on third parties who engage in personal information sale.

IV. Remove the Requirement to Respect Browser Signal Opt Outs so Consumers' Are Provided with Consumer Choice

The draft rules require businesses that collect personal information from consumers online to “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....”¹² This requirement is extralegal and goes beyond the text and scope of the CCPA by imposing a substantive new requirement on businesses that was not set forth by the legislature and does not have any textual support in the statute itself. For this reason and others we describe below, we ask the OAG to eliminate this requirement, or, at a minimum, give businesses the option to either honor browser plugins or privacy settings or mechanisms, or decline to honor such settings if the business includes a “Do Not Sell My Personal Information” link and offers another method for consumers to opt out of the sale of personal information.

The browser-based signal requirement in the proposed rules has no textual support in the CCPA itself. The California legislature could have included a browser-based signal mandate when it initially passed the CCPA, or when it amended it via multiple bills thereafter,¹³ but the legislature never chose to impose such a requirement. Moreover, the California legislature already considered imposing a similar browser setting requirement in 2013 when it amended the California Online Privacy Protection Act.¹⁴ The legislature ultimately decided against imposing a single, technical-based solution to enabling consumer choice and instead chose to offer consumers multiple avenues through which they may communicate their preferences. Together, these decisions reveal that the California legislature had the opportunity to enact a browser-based signal requirement on multiple occasions, but never chose to do so, and as such, the proposed regulation mandating that such signals be treated as verifiable consumer requests does not further legislative intent and is outside the scope of the CCPA.

If the OAG ultimately maintains this requirement, we suggest that the OAG modify it so that a business engaged in the sale of personal information must *either* abide by browser plugins or privacy settings or mechanisms, or may not honor such settings if the business includes a “Do Not Sell My Personal Information” link and offers another method for consumers to opt out of personal information sale by the business. The latter approach is more consistent with the spirit of the CCPA and the intentions of the legislature, as it affords consumers with robust choice and control over the sale of personal information. In contrast, browser-based signals or plugins would broadcast a single signal to all businesses opting a consumer out from the entire data

¹² *Id.* at § 999.315(c).

¹³ See AB 1121 (Cal. 2018); AB 25 (Cal. 2019); AB 874 (Cal. 2019); AB 1146 (Cal. 2019); AB 1355 (Cal. 2019); AB 1564 (Cal. 2019).

¹⁴ AB 370 (Cal. 2013).



marketplace. It is not possible through these settings for a consumer to make discrete choices among businesses allowing the consumer to restrict certain businesses while permitting other businesses to transfer data to benefit the consumer. Furthermore, it is not possible for a business to verify if a consumer set the browser setting or some intermediary did so without the authorization of the consumer.

In addition, certain intermediaries in the online ecosystem stand between consumers and businesses and therefore have the ability to interfere with the data-related selections consumers may make through technological choice tools. These intermediaries, such as browsers and operating systems, can impede consumers' ability to exercise choices via the Internet that may block digital technologies (*e.g.*, cookies, javascripts, and device identifiers) that consumers can rely on to communicate their opt out preferences. This result obstructs consumer control over data by inhibiting consumers' ability to communicate preferences directly to particular businesses and express choices in the marketplace. The OAG should by regulation prohibit such intermediaries from interfering in this manner.

We ask the OAG to eliminate the requirement to honor browser plugins or privacy settings or mechanisms, or, alternatively, revise the draft rules so that businesses have the option of honoring such settings or providing a "Do Not Sell My Personal Information" link along with another method for consumers to opt out of the sale of personal information by the business. We also ask the OAG to update the proposed rules to prohibit intermediaries from blocking or otherwise interfering with the technology used to effectuate consumer preferences in order to protect the opt out signals set by consumers via other tools.

V. Enable Effective Opt Out Mechanisms for Businesses that Do Not Maintain Personally Identifiable Personal Information

The proposed regulations require businesses to offer consumers a webform through which they may opt out of the sale of personal information.¹⁵ However, webforms may not work to facilitate opt outs for online businesses that do not maintain personally identifiable information about consumers. Many businesses in the online ecosystem may maintain personal information that does not identify a consumer on its own, for example, IP addresses, mobile advertising identifiers, cookie IDs, and other online identifiers. For businesses that maintain this non-identifying information, webforms may not work to facilitate consumer requests to opt out, because the consumer's submission of identifying information such as a name, email address, or postal address may not be easily matched to the non-personally identifiable information the business does maintain. This provision could undermine the privacy-protective elements of the CCPA by forcing companies to attempt re-identification techniques which are widely avoided by industry in its efforts to enhance consumer privacy.¹⁶ Consequently, the proposed rules should provide businesses with flexibility to offer mechanisms for consumers to opt out of personal information sale. The OAG has indicated it may issue another button or logo to enable a

¹⁵ Cal. Code Regs. tit. 11, § 999.315(a) (proposed Oct. 11, 2019).

¹⁶ See Fix CCPA, *Don't Force Companies to Connect Online Identities to Real Names*, located at <https://www.fixccpa.com/>.



consumer to opt out of the sale of personal information.¹⁷ We encourage the OAG to consider industry leading implementations that already have consumer recognition in crafting another acceptable opt out mechanism. We also ask the OAG to clarify that online businesses that do not maintain personally identifying information may use an effective method to enable a consumer to opt out other than a webform.

VI. Clarify Businesses Are Not Required to Collect or Maintain More Personal Information to Verify a Consumer

Pursuant to the draft regulations, “[a] business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes.”¹⁸ The AG should clarify by regulation that businesses are not required to collect data they do not maintain or collect in the regular course of business in order to verify a consumer’s identity.

Some businesses may maintain personal information in a manner that is not associated with a named actual person. For example, IP addresses and cookie IDs are kinds of personal information that could be associated with or linked to information from many consumers rather than information from a single consumer. Moreover, businesses often keep information that could identify a consumer’s identity separate from other information that may not be identifying on its own. This practice is privacy protective, as it separates consumer identities from certain information collected about the consumer. The draft rules’ current text could require businesses that do not maintain information that is associated with a named actual person to collect additional information from consumers in order to verify their identities. While the draft regulations acknowledge that “fact-based verification process[es]” may be required in such circumstances,¹⁹ this provision of the proposed regulations could force businesses to investigate consumer identities by procuring more data than they normally would in their normal course of business in order to verify consumers.

A business should not be required to obtain additional information from consumers in order to comply with the CCPA. The purpose of the law is to enhance privacy protections for consumers, and forcing businesses to collect data they would not otherwise collect, maintain, or normally associate with a named actual person has the potential to undermine consumer privacy rather than enhance it.²⁰ The OAG should clarify that while businesses *may* collect additional

¹⁷ Cal. Code Regs. tit. 11, at § 999.306(e) (proposed Oct. 11, 2019).

¹⁸ *Id.* at § 999.323(c).

¹⁹ *Id.* at 999.325(e)(2).

²⁰ For example, this mandate would force businesses to collect more information from consumers than they typically do in their normal course of business. Reports on the General Data Protection Regulation (“GDPR”) in Europe have revealed that unauthorized individuals can exploit the law to access personal information that does not



information from a consumer to verify the consumer's identity, the business does not need to do so to comply with the law.

VII. Ensure that Businesses May Provide User-Friendly Privacy Policies to Consumers

The proposed regulations set forth certain requirements for businesses in providing privacy-related notices to consumers. Some of these requirements, such as the obligation to provide relevant disclosures with respect to *each category of personal information collected*, represent new obligations that are not expressly included in the text of the CCPA and may force businesses to produce excessively long and confusing privacy notices that would do little to further consumers' understanding of business data practices. Other notice-related requirements in the draft rules are unclear. For example, the draft regulations do not clearly state whether the required notice at collection, notice of right to opt out, and notice of financial incentive may be provided to consumers in a privacy policy. We urge the OAG to update the draft rules so that consumers may receive understandable privacy notices and so that businesses may provide all required privacy-related notices in a single privacy policy disclosure.

According to the proposed regulations, in privacy policies business must list the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information “[f]or *each category of personal information collected*...”²¹ However, the terms of the CCPA itself do not require businesses to make disclosures relevant to each category of personal information collected, but rather require businesses to make disclosures with respect to all personal information collected. As such, requiring granular, category-by-category disclosures for each type of personal information collected imposes a significant new substantive requirement on businesses that has no textual basis for support in the CCPA.

Additionally, requiring granular disclosures for each category of personal information collected could impede businesses from ensuring privacy policies are “written in a manner that provides consumers [with] a meaningful understanding of the categories listed.”²² If businesses must make disclosures about sources, purposes, and third parties for each category of personal information collected, privacy notices could be excessively complicated, lengthy, and incomprehensible for consumers, thereby impeding the purpose of providing an informative and understandable consumer privacy notice. Moreover, consumers would be less likely to read and understand such lengthy notices, which could impede the CCPA's goal of enhancing the transparency of business data practices. The OAG should align the regulations with the text of the CCPA by removing the “for each category of personal information collected” language. This change would enable consumers to receive meaningful privacy policies that sensibly disclose

belong to them, causing risks of identity theft. See BBC News, *Black Hat: GDPR privacy law exploited to reveal personal data* (Aug. 9, 2019), located at <https://www.bbc.com/news/technology-49252501>.

²¹ Cal. Code Regs. tit. 11, § 999.308(b)(1)(d)(2) (proposed Oct. 11, 2019).

²² *Id.*



required information in an undaunting and clear format and would advance California legislators' aim of enabling comprehensible, workable consumer notices more effectively than requiring disclosures pertaining to each category of personal information collected.

VIII. Allow Businesses to Satisfy All CCPA-Related Notice Requirements in a Privacy Policy

Pursuant to the proposed rules, businesses must provide a privacy policy and certain other particular notices to consumers. Specifically, in addition to a privacy policy, businesses must provide a notice at collection, a notice of the right to opt out of the sale of personal information, and a notice of financial incentive.²³ However, the proposed rules do not clearly state whether the notice at collection, notice of the right to opt out of the sale of personal information, or notice of financial incentive may be offered to consumers through the privacy policy. The OAG should clarify that all required notices may be provided in a privacy policy.

The draft rules state that a notice at collection may be provided through a conspicuous link on the business's website homepage, mobile application download page, or on all webpages where personal information is collected, which represent typical methods through which privacy policies are normally offered to consumers.²⁴ However, the draft rules do not expressly confirm that a notice at collection may be provided through the privacy policy. Similarly, while a notice of the right to opt-out must include certain particular information or link to the section of the business's privacy policy that contains such information, there is no explicit confirmation that the opt out notice requirement may be satisfied by providing the necessary information in a privacy policy.²⁵ Finally, if a business offers a financial incentive or price of service difference online, the business must link to the section of the business's privacy policy that contains the required information, but it is unclear whether making such a disclosure counts as the required notice of financial incentive that must be offered to consumers.²⁶

We ask the OAG to update the proposed rules so they remove the requirement to provide disclosures with respect to each category of personal information collected, and so that they explicitly state that the notice at collection, notice of right to opt-out, and notice of financial incentive may be provided to consumers in a privacy policy. These updates would lessen the possibility for consumer notice fatigue by enabling more concise, readable notices. They would also be consistent with consumer expectations and would enable more effective and less confusing consumer disclosures, as all privacy-related information could be housed in a unified location. Moreover, such a rule would help businesses in their efforts to meet the CCPA's requirements, because business would be able to focus on reviewing and updating one notice as needed instead of multiple notices. The OAG should clarify that all required notices may be

²³ *Id.* at §§ 999.305, 306, 307.

²⁴ *Id.* at § 999.305(a)(2)(e).

²⁵ *Id.* at § 999.306(b)(1).

²⁶ *Id.* at § 999.307(a)(3).



provided in a privacy policy, because such a clarification would reduce confusion for consumers and better enable CCPA compliance for businesses.

IX. Clarify that Requesting Verifying Information from a Consumer Pauses the Time Period Within Which a Business Must Respond to the Request

The proposed regulations set forth a risk-based process by which businesses may engage in efforts to verify consumers before acting on their requests to delete and requests to know.²⁷ We support the non-prescriptive, risk-based framework for verifying consumer requests that is outlined in the proposed regulations. It provides businesses the flexibility they need to create verification mechanisms that fit their business models while being robust enough to accurately identify consumers submitting CCPA requests. However, despite the beneficial nature of the risk-based approach for verifying consumer requests that is outlined in the proposed rules, we are concerned that the draft rules do not provide businesses with enough time to verify consumers before they are responsible for effectuating CCPA requests.

The draft rules require a business to comply with requests to know and delete within 45 days of receiving the request regardless of the period of time it takes for the business to verify the request.²⁸ We ask the OAG to reconsider this requirement and update the draft rules so a business's request for information to verify a consumer's identity before effectuating a consumer request tolls or pauses the 45-day window within which the business must respond to the request. Consumer verification is necessary for businesses to accurately effectuate consumers' CCPA rights. Robust and accurate verification is in the interest of consumers, because without it, businesses run the risk of erasing or returning data that does not pertain to the requesting consumer. Such a result could have two distinct consumer harms: first, it would fail to fulfill the wishes of the consumer who actually submitted the request, and second, it could impact personal information about a consumer that did not make the request. Consequently, we urge the OAG to update the proposed rules so a business's request for verifying information tolls or pauses the 45-day period within which the business must respond to consumer requests to know and delete.

X. Clarify that a Business May Provide a General Toll-Free Number for Receiving CCPA Requests

According to the draft rules, a business must enable consumers to submit requests to know via a toll-free number and may provide a toll-free number to receive requests to delete and opt out of personal information sale. The proposed rules as currently drafted do not clarify if a business may offer its general toll-free number to receive CCPA requests or if a business must create a separate, CCPA-specific number through which it should receive consumer requests under the law. We ask the OAG to clarify that a business may offer consumers its general toll-free number to receive consumer CCPA requests and does not need to create or staff an entirely new phone number for such requests. Such an update to the proposed rules would decrease consumer confusion by funneling all business-related inquiries through one contact phone.

²⁷ *Id.* at §§ 999.323, 324, 325.

²⁸ *Id.* at § 999.313(b).



number. It would also help businesses by refraining from imposing an unnecessary cost on them to staff and maintain a separate number for CCPA requests. Consequently, we urge the OAG to update the draft rules to clarify that a business can provide its general consumer telephone number as the toll-free phone number through which it may receive consumer CCPA requests.

XI. Remove the Requirement to Flow Down Opt Out Requests to Third Parties to Whom the Business has Sold Personal Information in the Prior 90 Days

The proposed rules would require businesses to pass on the opt out requests they receive to third parties. Specifically, a business must “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.”²⁹ This requirement does not further meaningful consumer choice, as it takes a consumer’s opt out selection with respect to one business and propagates it throughout the ecosystem without the consumer’s express consent to do so. Furthermore, it represents a departure from the text of the CCPA by imposing a brand-new requirement on businesses that was not contemplated by the text of the law itself.

Requiring businesses to pass on opt out requests to third parties that received the consumer’s personal information in the prior 90 days could impede a consumer’s ability to exercise specific choices that are effective against particular businesses. A consumer’s choice to opt out of one business’s ability to sell personal information does not mean that the consumer meant to opt out of every business’s ability to sell personal information. This proposed rule has the potential to cause consumers to lose access to online offerings and content that they did not expect or choose to lose by submitting an opt out request to a single business. The law should not require businesses to understand a consumer’s opt out choice as a decision that must apply throughout the entire Internet ecosystem. In addition, requiring businesses to communicate opt out requests to third parties is a substantial new obligation that does not give businesses enough time to build processes to comply with the requirement before January 1, 2020.³⁰ The CCPA, as passed by the Legislature, already provides a means for consumers to control onward sales by third party businesses. The law requires that consumers be provided explicit notice and opportunity to opt out from sale.³¹ The new obligation to pass opt out requests on to third parties that received the consumer’s personal information within the past 90 days moves beyond the text and intent of the CCPA by imposing material and burdensome new obligations on businesses

²⁹ *Id.* at § 999.315(f).

³⁰ The Standardized Regulatory Impact Assessment (“SRIA”) analyzing the proposed regulations’ economic effect on the California economy is also deficient on this point. *See* SRIA at 25-26. The SRIA indicates “[t]he incremental compliance cost associated with this regulation is the extra work required by businesses to notify third parties that further sale is not permissible.” *Id.* at 25. This comment overlooks the ripple effect that the requirement to pass opt out requests on to third parties that have received a consumer’s personal information in the past 90 days would have throughout the Internet ecosystem and the economy. Under the draft rules, a consumer’s single opt out of sale request would restrict beneficial uses of personal information, including those generally occurring subsequent to the initial sale. The OAG should consider how restricting the sale of personal information by third parties in this way can “increase or decrease... investment in the state.” *See* Cal. Gov. Code § 11346.3(c)(1)(D).

³¹ Cal. Civ. Code § 1798.115(d).



without textual support in the CCPA. We therefore encourage the OAG to update the proposed rules so businesses are not required to pass opt out requests along to third parties. Alternatively, the OAG should limit the requirement to information the business actually sold to third parties in the previous 90 days.

XII. Align the Draft Rules with Consumer Choices by Removing the Requirement to Convert Unverifiable Requests to Delete into Requests to Opt Out

If a business cannot verify a consumer who has submitted a request to delete, the proposed rules would require the business to “inform the requestor that their identity cannot be verified and... instead treat the request as a request to opt out of personal information sale.”³² Compelling businesses to convert unverifiable consumer deletion requests into opt out requests could hinder or even completely impede meaningful consumer choice in the marketplace. This mandate has the potential to force a result that the consumer neither intended nor approved. Consequently, we ask the OAG to update the proposed rules so that businesses are not forced to transform unverified deletion requests into opt out requests unless the consumer specifically asks the business to do so.

The CCPA provides separate consumer rights for deletion and opting out of personal information sale because these two rights achieve different policy aims and consumer goals. While deletion is structured to erase the consumer’s personal information from the databases and systems *of the business to which the consumer communicates the request*, the opt out right empowers consumers to stop the transfer of data to *other businesses* in the chain. Because these two rights achieve two different objectives, the law should not compel consumers to opt out of personal information sale if a business cannot verify their request to delete. This outcome, which would be legally required by the proposed regulations, it is not likely to reflect the consumer’s desires in submitting a deletion request.

To illustrate this point, the OAG’s proposed rule requiring businesses to communicate opt out requests to third parties to whom they have sold personal information in the prior 90 days and instruct them not to further sell personal information could cause a consumer’s unverified deletion request to be transformed into an opt out request that is imposed on many other parties other than the business that is the recipient of the request. As a result, a business may be required to transform a deletion request a consumer may have thought she served on one business alone into an opt out request by that business and pass that opt out request along to other businesses without obtaining the consumer’s consent to take this action. This obligation therefore has the potential to unknowingly expose the consumer to potential loss of products and services she did not wish to lose. This result deprives consumers of the ability to make particularized selections about businesses who may and may not sell personal information. We therefore respectfully ask the OAG to align the draft rules with consumer choices by removing the requirement to convert unverifiable requests to delete into requests to opt out unless the consumer affirmatively requests that the business take such an action.

³² Cal. Code Regs. tit. 11, § 999.313(d)(1) (proposed Oct. 11, 2019).



* * *

Thank you for the opportunity to submit input on the content of the proposed regulations interpreting the CCPA. We look forward to continuing to engage with your office as it finalizes the draft rules. Please contact us with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
[REDACTED]

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
[REDACTED]

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[REDACTED]

Dave Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[REDACTED]

Alison Pepper
Senior Vice President
American Association of Advertising
Agencies, 4A's
[REDACTED]

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
[REDACTED]

CC: Mike Signorelli, Venable LLP



February 25, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Revised Proposed Regulations Implementing the California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the content of the February 10, 2020 release of revised proposed regulations implementing the California Consumer Privacy Act ("CCPA").¹ We appreciate the opportunity to continue to engage with the OAG on the important subject of consumer privacy and the implementing regulations that will help shape privacy protections in the state of California.²

We and our members strongly support protecting the privacy of Californians, and we believe consumer privacy deserves meaningful protection. We are encouraged by several updates the OAG made to the CCPA implementing regulations that will enhance consumer privacy and provide more clarity for businesses in their efforts to operationalize the law's terms. However, certain specific issues, which we address below in this letter, could be further clarified to help preserve consumers' ability to exercise meaningful choice in the marketplace and businesses' ability to provide products and services that consumers expect and value. We are also concerned that the quickly impending CCPA enforcement date of July 1, 2020 will leave little to no time for businesses to implement the changes the OAG has made to the draft regulations as well as any additional updates the OAG may make to the regulations before July of this year.

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend. Locally, our members are estimated to help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.³ Our members want to provide consumers with robust privacy protections while simultaneously maintaining their ability to do business in ways that benefit California's employment rate and its economy. We believe a regulatory scheme that enables strong individual privacy protections alongside continued economic development and advancement will best serve California consumers.

¹ See California Department of Justice, *Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File* (Feb. 10, 2020), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf?>.

² Our organizations submitted joint comments on the content of the OAG's original proposed rules implementing the CCPA. See *Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf> at CCPA 00000431 - 00000442.

³ IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <http://www.ana.net/getfile/23045>.

The requests we pose in this submission represent targeted suggestions to improve the CCPA implementing regulations for consumers and businesses alike. These comments are supplementary to filings that may be submitted separately and individually by the undersigned trade associations.

I. Afford Businesses Time to Update Their Practices in Light of Regulatory Revisions

Although the CCPA went into effect on January 1, 2020, the final regulations have not yet been promulgated, leaving our members and thousands of other California businesses uncertain concerning their ultimate compliance obligations. Given the extraordinary complexity of the law and the potential for other open issues to be clarified in subsequent updates to the draft rules, there will not be sufficient time for businesses to effectively implement the final regulations prior to the anticipated enforcement date of July 1, 2020. We therefore ask you to delay enforcement of the CCPA until January 2021 in order to provide businesses a sufficient time period to implement the new regulations before being subject to enforcement.

a. It Is Appropriate to Provide Businesses a Reasonable Period of Time to Implement the Regulatory Updates

As soon as the California Legislature passed the CCPA, it was clear that the law's requirements would evolve through both the legislative and rulemaking process. It was not clear, however, that key CCPA provisions would be substantially amended so close to its effective date, and that the rules implementing its terms would not be finalized until after the law became operative.

While we recognize that the amendments in the California Legislature delayed the development and formal release of draft regulations implementing the CCPA until October 11, 2019,⁴ these draft rules presented significant new and unprecedented requirements, such as entirely new recordkeeping obligations, notice requirements, and verification rules, among many other novel obligations.⁵ Then, on February 10, 2020, the rules changed again, altering the requirements businesses had used to build systems, processes, and policies for the CCPA. Businesses are contending with the proposed regulations' new mandates from both the October 11, 2019 and February 10, 2020 release of draft rules, and they are working earnestly to adjust their systems and build new processes to facilitate compliance.

Unfortunately, it is presently unclear when the rules will be finalized and whether they will be further amended. Just mere months before enforcement is scheduled to begin, companies that are subject to the CCPA are faced with the possibility that the draft rules could substantially change again and impose other entirely new requirements and nuances on businesses. If the rules change again, the OAG must issue a new notice in the California Regulatory Notice Register and provide for another comment period of 15 to 45 days.⁶ The rules will not be effective until they are submitted and reviewed by the Office of Administrative Law, further reducing the time available to businesses to implement the regulations. This timeline increases the likelihood that the draft rules will not be finalized before, or only a short period prior to the law's July 1, 2020 enforcement date.

We and our members strongly support the underlying goals of the CCPA. The limited and quickly shrinking time before the existing enforcement deadline, however, will place businesses in a nearly untenable position. Without final regulatory requirements, businesses will be unable to make operational changes to their systems, further delaying finalization of their compliance programs. Businesses should be

⁴ See State of California Office of Administrative Law, *Notice Publication/Regulations Submission* (Oct. 11, 2019), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-std400a.pdf>.

⁵ Cal. Code Regs. tit. 11, § 999.305-308, 317, 323-325 (proposed Feb. 10, 2020).

⁶ See Office of the Attorney General, California Department of Justice, *California Consumer Privacy Act (CCPA): Background on Rulemaking Process* at 3, located at https://oal.ca.gov/rulemaking_participation.

afforded an appropriate time period to implement the new regulations once they become final and before being subject to enforcement.

b. Providing a Reasonable Period of Time for Implementing the New Regulations Benefits Consumers

While the law instructs the OAG not to bring any enforcement action prior to July 1, 2020, there is no restriction on you providing a reasonable period of additional time for California businesses to review and implement the final regulations before your office initiates any enforcement actions.⁷ Thus, in order to avoid consumer and business confusion with respect to the new rules, we request that you delay enforcement of the law to begin in January 2021. This short deferral will give businesses the time they need to understand and effectively operationalize the rules helping ensure consumers have access to the rights afforded under the new law.

Business attempts to comply with an incomplete legal regime risk causing significant consumer frustration and the implementation of inadequate or duplicative compliance tools. While we understand that your office is working expeditiously to provide clear rules for businesses to operationalize the CCPA, the clock is working against well-intentioned businesses in their compliance efforts. We urge you to give California business the opportunity to understand what is required under the law before they are at risk for being penalized for violating its terms.

While our members support California's intent to provide consumers enhanced privacy protections, the evolving nature of the CCPA and the draft nature of the proposed rules make the current enforcement date of July 1, 2020 a difficult deadline for businesses and consumers alike. Consumer privacy is best served when businesses that leverage data do so in accordance with clear and concrete laws and regulations that present them with adequate time to adjust their practices to come into compliance with new requirements.

We urge you to provide a moratorium on enforcement until January 2021, thereby giving businesses throughout the United States that operate in California adequate time to prepare to adhere to the law's final form. Delaying the CCPA's enforcement in this manner will help ensure that businesses can effectively provide consumers with the new protections and rights that the law and its implementing regulations require.

II. Enable Consumer Choice By Removing the Requirement to Honor Browser Settings and Global Privacy Controls

The revised proposed rules require businesses that collect personal information from consumers online to treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism that signals the consumer's choice to opt out of the sale of personal information, as a valid request submitted for that browser, device, or consumer.⁸ In our prior submission to the OAG, we explained that this requirement robs consumers of the ability to exercise granular choice. This mandate would obstruct consumers' individualized, business-by-business decisions about entities that can and cannot engage in the sale of personal information. Moreover, this requirement represents an obligation that has no support in the text of the CCPA itself and extends far beyond the likely intent of the California Legislature in passing the law. For these reasons, we renew our request for the OAG to remove the requirement to respect user-enabled global privacy controls, or, at a minimum, to give businesses the

⁷ Cal. Civ. Code § 1798.185(c).

⁸ Cal Code Regs. tit. 11, § 999.315(d) (proposed Feb. 10, 2020).

option to honor user-enabled global privacy controls or decline to honor such settings if the business offers another, equally effective method for consumers to opt out of personal information sale.

The requirement to honor user-enabled global privacy controls is a substantive obligation that the California Legislature did not include in the text of the CCPA itself. Despite numerous amendments the legislature passed to refine the CCPA, none of them included a mandate to honor browser signals or global privacy controls. Additionally, the California Legislature considered a similar requirement in 2013 when it amended the California Online Privacy Protection Act, but it declined to impose a single, technical-based solution to address consumer choice and instead elected to offer consumers multiple ways to communicate their preferences to businesses.⁹ The revised proposed rules' imposition of a requirement to honor user-enabled privacy controls would result in broadcasting a single signal to all businesses opting a consumer out from the entire data marketplace. This requirement would obstruct consumers' access to various products, services, and content that they enjoy and expect to receive.

Additionally, requiring businesses to honor global, single-signal privacy control opt out choices would effectively convert the CCPA's statutorily mandated opt out regime to an opt in regime. Because businesses would be required to respect a user-enabled global privacy control opt out setting under the draft rules, they would be forced to approach consumers on an individualized basis to ask them to opt in to personal information sale after receiving a user-enabled global privacy setting opt out through a browser. This outcome is certainly not the result the California Legislature intended in passing the CCPA, which clearly proposes an opt out approach to consumer data sales rather than an opt in approach.¹⁰

In the most recent iteration of the draft rules, the OAG added provisions to the requirement that allow a business to notify a consumer of a conflict between any business-specific privacy setting or financial incentive and a global privacy control.¹¹ According to the updated regulations, a business may give the consumer a choice to confirm the business-specific setting or the global privacy control.¹² However, the draft rules still require a business to "respect the global privacy control," thereby forcing businesses to act on global privacy settings before they can confirm whether the consumer actually wanted to make a choice to end beneficial transfers of data that occur via the Internet.¹³ This option, therefore, does nothing to further a consumer's actual desired or expressed choices. The fact that the rules now allow for a business to confirm a consumer's intentions does little to save the consumer from unintentionally losing access to various products, services, and valuable content through the Internet. Additionally, this provision stands to advantage certain players in the market that have a direct relationship with consumers. Businesses that do not directly interact with consumers online, such as third-party entities, would not have the ability to confirm whether a consumer intended to apply a browser signal or privacy setting to the entire Internet or whether the consumer would rather abide by the choice the consumer made with respect to that particular business.

The revised proposed rules also note that a privacy control "shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings."¹⁴ Although this new provision reduces the potential for default settings to miscommunicate consumers' actual preferences, it does not address the fact that intermediaries in the online ecosystem stand between consumers and businesses and have the ability to interfere with the data-related selections consumers may make through technological choice tools. Obligating businesses to honor user-enabled privacy settings

⁹ See AB 370 (Cal. 2013).

¹⁰ Cal. Civ. Code § 1798.120.

¹¹ Cal. Code Regs. tit. 11, § 999.315(d)(2) (proposed Feb. 10, 2020).

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.* at § 999.315(d)(2).

that are presented to consumers through an intermediary vests power in the hands of the intermediary and risks inhibiting consumers' ability to communicate preferences directly to particular businesses. It also makes intermediary meddling in consumers' expressed privacy choices harder to detect, especially if a consumer makes a choice directly with a business that conflicts with a global opt-out signal set by a browser.

To preserve consumers' ability to exercise granular choices in the marketplace, to keep the regulations' requirements in line with legislative intent in passing the CCPA, and to reduce entrenchment of intermediaries and browsers that have the ability to exercise control over user-enabled privacy settings, we ask the OAG to remove the requirement to honor user-enabled privacy controls. Alternatively, we ask the OAG to update the draft rules so a business may *either* honor user-enabled privacy controls or decline to honor such settings *if* the business provides another equally effective method for consumers to opt out of personal information sale, such as a "Do Not Sell My Personal Information" link.

III. Clarify Financial Incentive Terms So Californians May Continue to Benefit from Consumer Loyalty Programs

The OAG did not take steps to materially clarify the draft rules' financial incentive requirements in its revisions to the proposed regulations. Without additional clarity on this issue, loyalty programs offered in California could be significantly undermined due to business confusion regarding how to implement the regulatory mandates. We respectfully ask the OAG to clarify or remove the rules' ambiguous terms requiring businesses to ensure that financial incentives are reasonably related to the value of a consumer's data. We also ask the OAG to clarify or remove the requirement to disclose an estimate of the value of the consumer's data as well as the method of calculating such value in a notice of financial incentive.

According to the revised proposed rules, "[i]f a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference."¹⁵ Despite this mandate, the draft rules do not provide any helpful information regarding how a business may justify that a price or service difference is reasonably related to the value of a consumer's data. The revised proposed regulations also do not address how businesses may reasonably quantify nontangible value in terms of fostering consumer loyalty and goodwill.

Californians greatly benefit from loyalty and rewards programs and the price differences and discounts they receive for participating in those programs. Loyalty programs exist due to consumers' widespread participation in such programs. Without consumer data, loyalty programs would not be possible. Consumer data increases businesses' access to useful information as well as their ability to generate revenue by marketing their products and services. Allowing consumers to continue to participate in loyalty programs without providing personal information to the business would defeat the purposes of the programs. Consumers who opt out or delete personal information from the loyalty program would essentially be permitted a "free ride" on the program, reaping all of its benefits due to data provided by other consumers. Additionally, it is not immediately apparent how any business can ensure that the program is "reasonably related to the value of the consumer's data." The lack of clarity on this issue and the "free rider" problem enabled by the draft regulations could cause many businesses to decline to continue offering loyalty programs to California residents.

Moreover, the requirement to disclose an estimate of the value of the consumer's data as well as the method of calculating such value in a notice of financial incentive represents a particularly onerous

¹⁵ *Id.* at § 999.336(b).

requirement that would engender consumer confusion and could have anticompetitive effects.¹⁶ Businesses typically offer multiple discounts to consumers through loyalty programs at one time. Requiring businesses to disclose an estimate of the value of the consumer's data and the method of calculating such value would inundate and confuse consumers with multiple and potentially duplicative privacy notices and would provide no tangible consumer benefit. Additionally, disclosing such information in a privacy notice could reveal confidential information about a business and pose risks to the business's competitive position in the market. Forcing businesses to reveal internal and proprietary valuations of data could negatively impact competition and could impose significant risks to business proprietary information.

For the foregoing reasons, we respectfully ask the CA AG to clarify or remove the unreasonably onerous financial incentive requirements inherent in the revised rules. In particular, we ask the OAG to clarify or remove the provisions requiring businesses to disclose a good faith estimate of the value of the consumer's data, disclose their methods of calculating such value, and ensure that financial incentives offered through loyalty programs are reasonably related to the value of the consumer's data. These requirements are particularly unclear and therefore could be impossible to operationalize. Without additional clarity, the draft rules' financial incentive terms could inhibit or drastically reduce the availability of loyalty programs offered in the state.

* * *

Thank you for the opportunity to submit input on the content of the revised proposed regulations implementing the CCPA. We look forward to continuing to engage with the OAG as it takes steps to finalize the draft rules. Please contact Mike Signorelli of Venable LLP at [REDACTED] with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Senior Vice President
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

¹⁶ *Id.* at § 999.307(b)(5).



March 27, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Second Set of Proposed Regulations Implementing the California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the proposed regulation included in 999.315(d) of the March 11, 2020 release of the second set of modifications to the text of the proposed regulations implementing the California Consumer Privacy Act ("CCPA").¹ This requirement exceeds the scope of the OAG's ability to regulate in conformance with the CCPA, runs afoul of free speech rights inherent in the United States Constitution, and impedes the ability of consumers to exercise granular choices in the marketplace. We ask that it be struck or modified per the below comment.

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend. Locally, our members are estimated to help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.² We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous submissions and in the sections that follow below, the draft regulations implementing the law could be updated to better enable consumers to exercise meaningful choices and to help businesses in their efforts to continue to provide value to California's consumers and its economy.³

Despite businesses' best efforts to develop compliance strategies for the CCPA, current events coupled with the unfinalized nature of the draft rules stand in the way of entities' earnest work to facilitate compliance with the law. As we have discussed in our prior submissions, the draft rules' onerous terms concerning global controls and browser settings stand to impede consumer choices as well as access to various products, services, and content in the digital ecosystem. More urgently, the novel coronavirus known as COVID-19 has shaken businesses' standard operating procedures as well as the development of policies, processes, and systems for the CCPA. In this period of crisis facing the world-at-large, entities should be focused on dedicating funds, time, and efforts to supporting their employees and the response to

¹ See California Department of Justice, *Notice of Second Set of Modifications to Text of Proposed Regulations* (Mar. 11, 2020), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-second-mod-031120.pdf?>

² IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <http://www.ana.net/getfile/23045>.

³ Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG's proposed rules implementing the CCPA. See *Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf> at CCPA 00000431 - 00000442; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-15-day-comments-022520.pdf> at CCPA_15DAY_000554 - 000559.

the coronavirus outbreak rather than diverting resources to prepare for an ever-evolving set of regulations under the CCPA. Therefore, we support the request made earlier this month by a group of sixty-six (66) trade associations, organizations, and companies to your office asking you to delay enforcement until January 2, 2021.⁴

Our members are committed to offering consumers robust privacy protections while simultaneously maintaining their ability to support California's employment rate and its economy in these unprecedented times as well as access to ad-funded news. We believe a regulatory scheme that enables strong individual privacy protections alongside continued economic development and advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA implementing regulations for Californians as well as the global economy.⁵

I. Give Businesses the Option to Honor Browser Settings and Global Controls

The revised proposed rules require businesses that collect personal information from consumers online to treat user-enabled global controls, such as a browser plugin or setting, device setting, or other mechanism that purports to carry signals of the consumer's choice to opt out of the sale of personal information, as a valid request submitted for that browser, device, or consumer.⁶ This requirement exceeds the scope of the OAG's authority to regulate pursuant to the CCPA, runs afoul of free speech rights inherent in the United States Constitution, and impedes consumers of the ability to exercise granular choices in the marketplace. For these reasons, we ask the OAG to remove this requirement, or, at a minimum, to give businesses the option to honor such controls or decline to honor such settings if the business offers another, equally effective method for consumers to opt out of personal information sale.

a. The Browser Setting and Global Control Mandate Exceeds the OAG's Regulatory Authority Pursuant to the CCPA

Requiring businesses to honor such controls and browser settings is an obligation that has no support in the text of the CCPA itself and extends far beyond the intent of the California Legislature in passing the law. Under California administrative law, when an agency is delegated rulemaking power, rules promulgated pursuant to that power must be "within the lawmaking authority delegated by the Legislature," and must be "reasonably necessary to implement the purposes" of the delegating statute.⁷ The CCPA gives the OAG power to "adopt regulations to further the purposes of [the CCPA]," but not to adopt regulations that contravene the framework set up by the Legislature when it passed the law.⁸

The CCPA was plainly structured to provide consumers with the right to opt out of sales of personal information.⁹ However, the requirement to respect the proposed controls and browser settings effectively transforms the CCPA's opt-out regime into an opt-in regime by enabling intermediaries to set opt-out signals through browsers that apply a single signal across the entire Internet marketplace. Individual businesses will consequently be forced to ask consumers to opt in after receiving a global opt-out signal set by an intermediary, thereby thwarting the granular opt-out structure the California Legislature purposefully enacted in passing the CCPA. The OAG's regulation mandating that businesses

⁴ *Joint Industry Letter Requesting Temporary Forbearance from CCPA Enforcement* (Mar. 20, 2020), located at <https://www.ana.net/getfile/29892>.

⁵ These comments are supplementary to filings that may be submitted separately and individually by the undersigned trade associations.

⁶ Cal Code Regs. tit. 11, § 999.315(d) (proposed Mar. 11, 2020).

⁷ *Western States Petroleum Assn. v. Bd. of Equalization*, 304 P.3d 188, 415 (Cal. 2013) (quoting *Yamaha Corp. of America v. State Bd. Of Equalization*, 960 P.2d 1031 (Cal. 1998)).

⁸ Cal. Civ. Code § 1798.185.

⁹ *Id.* at § 1798.120.

obey such controls and browser signals therefore exceeds the scope of the OAG's authority to issue regulations under the CCPA.

The requirement to obey such controls is a substantive obligation that the California Legislature did not include in the text of the CCPA itself. Despite numerous amendments the legislature passed to refine the CCPA, none of them included a mandate for browser signals or global controls. Additionally, the California Legislature considered a similar requirement in 2013 when it amended the California Online Privacy Protection Act ("CalOPPA"), but it declined to impose a single, technical-based solution to address consumer choice and instead elected to offer consumers multiple ways to communicate their preferences to businesses.¹⁰ The Legislature did not intend to institute a requirement to mandate global controls or browser signals when it amended CalOPPA in 2013, and it similarly did not intend to do so when it passed the CCPA in 2018. The obligation to honor such signals in the draft rules therefore thwarts legislative intent and is an impermissible exercise of the OAG's ability to issue regulations under the law.

b. The Browser Setting and Global Control Mandate Contravenes Constitutional Rights to Free Speech

The OAG's proposed rule regarding such controls and browser signals violates the First Amendment to the United States Constitution by converting the CCPA's opt-out structure into a de facto opt-in structure and by improperly restricting free speech. Businesses' dissemination of the data they collect constitutes constitutionally protected commercial speech.¹¹ A regulation restricting commercial speech is unconstitutional unless the state has a substantial interest in restricting this speech, the regulation directly advances that interest, and the regulation is narrowly tailored to serve that interest.¹² While there may be a substantial state interest in protecting consumer privacy,¹³ the OAG's directive to respect such controls and browser settings does not advance the government's substantial interest. Moreover, this rule is not narrowly tailored to advance such an interest. The regulatory requirement therefore violates the First Amendment.

Commercial speech is entitled to protections under the United States Constitution. Regulations that provide "ineffective or remote support for the government's purpose" impermissibly burden constitutional protections afforded to commercial speech.¹⁴ The wide-ranging opt-out structure set forth by the California Legislature and the OAG particularly focus on a consumer's relationship with an individual business. This structure enables consumers to express opt-out preferences in the context of their unique relationships with individual entities. By contrast, the global controls mandate obligates businesses to figure out consumers' individual preferences regarding data disclosures from a singular browser setting. Moreover, requiring businesses to defer to such controls as a way to understand consumers' true preferences is less effective and less direct than the opt-out methods employed by the rest of the OAG's regulations. If the state's interest is in stopping the disclosure of specific data that a consumer wishes to restrict from sale, such a proposal does not adequately further this aim. It provides no way for businesses

¹⁰ See *Assembly Committee on Business, Professions and Consumer Protection*, Hearing Report on AB 370 (Cal. 2013) (Apr. 16, 2013), located at

https://leginfo.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201320140AB370# ("According to the California Attorney General's Office, 'AB 370 is a transparency proposal – not a Do Not Track proposal. When a privacy policy discloses whether or not an operator honors a Do Not Track signal from a browser, individuals may make informed decisions about their use of the site or service.'")

¹¹ See *Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001); *Boetler v. Advance Magazine Publishers Inc.*, 210 F. Supp. 3d 579, 597 (S.D.N.Y. 2016).

¹² *Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).

¹³ *Verizon Northwest, Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1192 (W.D. Wash.).

¹⁴ *Id.* (quoting *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980)).

to divine that a consumer wishes to keep personal information within the confines of a specific business relationship, and instead compels businesses to guess at consumers' preferences from an indirect signal that may not accurately reflect a consumer's wishes.

In addition, the AG's proposed rule is not narrowly tailored to serve the state's interest. Instead, it senselessly restricts the commercial speech of businesses without supporting the efficacy of the existing opt-out framework. Narrowly tailored regulations are not disproportionately burdensome. Additionally, they must "signify a careful calculation of the costs and benefits associated with the burden on speech imposed."¹⁵ The existing opt-out regime implemented by the California Legislature offers businesses more exact information about specific, granular preferences of individual consumers than the global controls mandate. The global controls requirement serves no purpose that is not already served by existing opt-out rules in the draft regulations and the law itself, and it could potentially restrict speech by requiring businesses to act on inaccurate information about a consumer's individual preferences.

The proposed regulations note that businesses may contact consumers to ascertain their true intent regarding personal information sales if a global control conflicts with a choice the consumer individually set with the business. However, the rules require the business to defer to the global controls in the meantime, thus mandating a potentially incorrect expression of user preferences at the expense of specific choices the consumer indicated to the contrary. In addition, businesses bear the burden of ascertaining the consumer's true intent after receiving a global signal that does not align with an individual consumer's preferences. In contrast, the opt-out privacy framework set forth in the CCPA itself and bolstered by the draft rules is both more precise and less burdensome. It enables businesses to assess specific preferences of users in the context of each unique consumer relationship, and it restricts commercial speech only if that speech is known to contravene consumer preferences. The global controls mandate consequently does not further the goals of the existing framework, but it does needlessly restrict commercial speech. The global controls rule therefore does not pass constitutional muster because it burdens commercial speech without appropriately balancing those burdens with benefits.

c. The Browser Setting and Global Control Mandate Impedes Consumer Choice

The revised proposed rules' imposition of a requirement to honor such controls would result in broadcasting a single signal to all businesses, opting a consumer out from the entire online ecosystem. This requirement would obstruct consumers' access to various products, services, and content that they enjoy and expect to receive, and it would thwart their ability to exercise granular, business-by-business selections about entities that can and cannot sell personal information in the digital marketplace.

In the March 11, 2020 updates to the draft rules, the OAG removed the requirement for a consumer to "affirmatively select their choice to opt-out" and the requirement that global controls "shall not be designed with any pre-selected settings."¹⁶ The removal of these provisions entrench intermediaries in the system and will advantage certain business models over others, such as models that enable direct communications between consumers and businesses. It will also enable intermediaries to set *default* signals through browsers without consumers having to approve of them before they are set. This outcome risks causing businesses to take specific actions with respect to consumer data that the consumer may not want or intend. The OAG should take steps to ensure that default privacy signals may not be set by intermediaries without the consumer approving of the signals set and the choices they relay to businesses.

Moreover, the draft rules do not address how businesses should interpret potentially conflicting signals they may receive directly from a consumer and through a global control or a browser setting. For

¹⁵ *Id.* at 1194.

¹⁶ Cal. Code Regs. tit. 11, § 999.315(d)(2) (proposed Mar. 11, 2020).

example, if a business directly receives a consumer's permission to "sell" personal information, but later receives a global control signal through a browser set by default that indicates the consumer has opted out of such sales, which choice should the business follow? The CCPA itself allows businesses to contact consumers asking them to opt in to personal information sales after receiving opt-out signals only once in every twelve month period.¹⁷ As such, the business's ability to communicate with the consumer to ascertain their true intentions may be limited despite the draft regulations' statement that a business may notify consumers of conflicts between setting and give consumers the choice to confirm the business-specific setting.

To preserve consumers' ability to exercise granular choices in the marketplace, to keep the regulations' requirements in line with constitutional requirements and legislative intent in passing the CCPA, and to reduce entrenchment of intermediaries and browsers that have the ability to exercise control over settings, we ask the OAG to remove the requirement to obey such controls. Alternatively, we ask the OAG to update the draft rules so a business may *either* honor user-enabled privacy controls or decline to honor such settings *if* the business provides another equally effective method for consumers to opt out of personal information sale, such as a "Do Not Sell My Personal Information" link.

* * *

Thank you for the opportunity to submit input on the content of the revised proposed regulations implementing the CCPA. Please contact Mike Signorelli of Venable LLP at [REDACTED] with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Senior Vice President
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

Lou Mastria
Executive Director
Digital Advertising Alliance

¹⁷ Cal. Civ. Code § 1798.135(a)(5).



October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Third Set of Proposed Modifications to Text of California Consumer Privacy Act Regulations

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the third set of proposed modifications to the text of the California Consumer Privacy Act ("CCPA") regulations.¹

As explained in more detail below, the OAG's proposed modifications: (1) unreasonably restrict consumers from receiving important information about their privacy choices, (2) prescriptively describe how businesses must provide offline notices, and (3) unfairly fail to hold authorized agents to the same consumer notice standards as businesses. The OAG's potential changes to Section 999.315 would inhibit consumers from receiving transparent information and impinge on businesses' right to free speech. In addition, the proposed modifications to Section 999.326 would not provide any protections for consumers related to their communications with authorized agents, as such agents are not presently held to similar consumer notice rules as businesses. Finally, the OAG's proposed edits to Section 999.306 could stymie the flexibility businesses need to provide effective offline notices to consumers. We consequently ask the OAG to strike or modify the modifications per the below comments.

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising expenditures. Locally, our members are estimated to help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.² We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous comment submissions and in the sections that follow below, the draft regulations implementing the law should be updated to better enable consumers to exercise informed choices and to help businesses in their efforts to continue to provide value to California consumers while also supporting the state's economy.³

¹ See California Department of Justice, *Notice of Third Set of Proposed Modifications to Text of Regulations* (Oct. 12, 2020), located at <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-third-mod-101220.pdf?>

² IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <http://www.ana.net/getfile/23045>.

³ Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG's proposed rules implementing the CCPA. See *Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA 00000431 - 00000442; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-15day-comments-set1.pdf> at CCPA_15DAY_000554 - 000559; *Second Set of Proposed Regulations Implementing the California*

Our members are committed to offering consumers robust privacy protections while simultaneously providing access to ad-funded news, apps, and a host of additional online services. These offerings we have all become much more dependent on in recent months with the widespread proliferation of the COVID-19 pandemic. Ad-supported online content services have been available to consumers and will continue to be available to consumers so long as laws allow for innovation and flexibility without unnecessarily tilting the playing field away from the ad-subsidized model. The most recent modifications to the CCPA regulations set forth a prescriptive interpretation of the CCPA that could limit our members' ability to support California's employment rate and its economy in these unprecedented times. We believe a regulatory scheme that offers strong individual privacy protections and enables continued economic advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA regulations for Californians as well as the economy.

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

The U.S. economy is fueled by the free flow of data. Throughout the past three decades of the commercial Internet, one driving force in this ecosystem has been data-driven advertising. Advertising has helped power the growth of the Internet by delivering new, innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this responsible advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.⁴ This means that the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.⁵

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. In a September 2020 survey conducted by the Digital Advertising Alliance, 93 percent of consumers stated that free content was important to the overall value of the Internet and more than 80 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.⁶ The survey also found that consumers estimate the personal value of ad-supported content and services on an annual basis to be \$1,403.88, representing an increase of over \$200 in value since 2016.⁷ Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored

Consumer Privacy Act, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA_2ND15DAY_00309 - 00313.

⁴ John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), located at <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

⁵ *Id.*

⁶ Digital Advertising Alliance, *SurveyMonkey Survey: Consumer Value of Ad Supported Services – 2020 Update* (Sept. 28, 2020), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf.

⁷ *Id.*

experience, and research demonstrates that they are generally not reluctant to participate online due to data-driven advertising and marketing practices.

Without access to ad-supported content and online services, many consumers would be unable or unwilling to participate in the digital economy. Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁸ The ad-supported Internet therefore offers individuals a tremendous resource of open access to information and online services. Without the advertising industry's support, the availability of free and low-cost vital online information repositories and services would be diminished. We provide the following comments in the spirit of preserving the ad-supported digital and offline media marketplace that has provided significant benefit to consumers while helping to design appropriate privacy safeguards to provide appropriate protections for them as well.

II. The Regulations Should Support Consumers' Awareness of the Implications of Their Privacy Decisions, Not Hinder It in Violation of the First Amendment

The proposed online and offline modifications unreasonably limit consumers' ability to access accurate and informative disclosures about business practices as they engage in the opt out process. Ultimately, this restriction on speech would not benefit consumers or advance a substantial interest. The proposed rules state: "Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request."⁹ This language unduly limits consumers from receiving important information as they submit opt out requests. It is also overly limiting in the way that businesses may communicate with consumers. As highlighted above, data-driven advertising provides consumers with immensely valuable digital content for free or low-cost, as well as critical revenue for publishers, by increasing the value of ads served to consumers. As the research cited above also confirms, consumers have continually expressed their preference for ad-supported digital content and services, rather than having to pay significant fees for a wide range of apps, websites, and internet services they use. However, as a result of the proposed modifications, consumers' receipt of factual, critical information about the nature of the ad-supported Internet would be unduly hindered, thereby undermining a consumer's ability to make an informed decision. A business should be able to effectively communicate with consumers to inform them about how and why their data is used, and the benefit that data-driven advertising provides as a critical source of revenue.

It is no secret that consumers greatly value the information they can freely access online from digital publishers. However, local news publishers, for instance, continue to struggle to get readers to pay subscription fees for their content, even though this content is highly valuable to consumers and society. Thus, most news publishers have become increasingly reliant on tailored advertising, because it provides greater revenue than traditional advertising. However, the proposed modifications, as drafted, could obstruct consumers from receiving truthful, important information by hindering a business' provision of a reasonable notice to consumers about the funding challenges opt outs pose to their business model.

The CCPA regulations should not prevent consumers from receiving and businesses from providing full, fair, and accurate information during the opt out process. The proposed modification would

⁸ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

⁹ Cal. Code Regs. tit 11, § 999.315(h)(3) (proposed Oct. 12, 2020).

impede consumers from receiving important information about their privacy choices, such as information about the vital nature of the ad-supported Internet as described in Section I, and, as explained in Section III, they may be contemporaneously receiving partial or misleading negative information about their opt out rights.

To ensure a fully informed privacy choice, consumers must have every ability to access information about business practices and the benefits of the digital advertising ecosystem. Providing ample and timely opportunities for consumers to gain knowledge about their choice to opt out is of paramount importance to avoid confusion and ignorance; this allows a consumer to be fully informed about the actual implications of their decision. By prohibiting a business from requiring a consumer to “to click through or listen to reasons why they should not submit a request to opt-out *before* confirming their request” the regulations do not safeguard against this concern. As presently written, the proposed modification appears to limit businesses’ ability to provide such vital information as a consumer is opting out, even if such information is presented in a seamless way. It is unclear what amount of information, or what method in which such information is presented, could constitute a violation of the rules. Instead of setting forth prohibitive rules that could reduce the amount of information and transparency available to consumers online, the OAG should prioritize facilitating accurate and educational exchanges of information from businesses to consumers. As a result, we ask the OAG to revise the text of the proposed modification in Section 999.315(h)(3) so that businesses are permitted to describe the impacts of an opt out choice while facilitating the consumer’s request to opt out.

Additionally, the restrictions created by this proposed modification infringe on businesses’ First and Fourteenth Amendment right to commercial speech. As written, Section 999.315(h)(3) restricts the information consumers can receive from businesses as they submit opt out requests by limiting the provision of accurate and truthful information to consumers. The Supreme Court has explained that “people will perceive their own best interest if only they are well enough informed, and . . . the best means to that end is to open the channels of communication, rather than to close them. . . .”¹⁰ Because this proposed regulation prescriptively regulates channels of communication, it violates the First and Fourteenth Amendments.

The state may not suppress speech that is “neither misleading nor related to unlawful activity” unless it has a substantial interest in restricting this speech, the regulation directly advances that interest, and the regulation is narrowly tailored to serve that interest.¹¹ The proposed regulation fails each part of the test:

- **No substantial interest:** Although there is no stated justification in the proposal, the most likely interest would be to streamline opt out requests by making it easier and faster to submit opt-outs. The OAG presumably wants nothing to impede consumers from opting out, but it is unclear because the OAG has not affirmatively stated its purpose for the proposed modification. Consumers should be made aware of the ramifications of their opt out decisions as they are opting out – not after confirming a request – so they do not make opt out choices to their detriment because they do not know the effect of such choices. For this reason, they should be able to receive information from businesses about the consequences of their opt out choices as they are submitting opt out requests. Providing information concerning the impact of an opt out is not an impediment to the process, but rather improves it.

¹⁰ *Virginia Pharmacy Board v. Virginia Citizens Consumer Council*, 425 U. S. 748, 770 (1976).

¹¹ *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980); *see also Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).

- ***No advancement of the interest:*** If streamlining opt out requests to remove perceived impediments is the justification for the proposed rule, then the proposal does not advance that interest. The proposed regulation already includes many other specific requirements that facilitate speed and ease of opt-outs, including a requirement to use the minimal number of steps for opt-outs (and no more than the number of steps needed to opt in), prohibiting confusing wording, restricting the information collected, and prohibiting hiding the opt-out in a longer policy, all of which directly advance this interest without suppressing speech. The proposed rule limiting businesses from clicking through or listening to reasons would not make the opt out process easier for consumers, because it could result in consumers making uninformed choices if they are not notified of the consequences of their decision to opt out as they are making it. A “regulation may not be sustained if it provides only ineffective or remote support for the government’s purpose.”¹² This proposed regulation is both ineffective and provides no support for the government’s purpose.
- ***Not narrowly tailored:*** The proposed regulation is an overly broad and prescriptive restriction on speech that hinders accurate and educational communications to consumers about the consequences of a decision to opt-out. The regulations already include various other provisions that work to streamline the opt out process. “[I]f the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.”¹³ As noted above, there are many ways to craft regulations to require simple and fast opt-out mechanisms that do not suppress lawful and truthful speech.

In sum, the regulation violates each and every prong of the framework for evaluating commercial speech. “As in other contexts, these standards ensure not only that the state’s interests are proportional to the resulting burdens placed on speech but also that the law does not seek to suppress a disfavored message.”¹⁴ The proposed regulation would do exactly that. Thus, it is a content-based restriction on speech, subject to heightened scrutiny. The OAG should revise the text of the proposed modification in Section 999.315(h)(3) to avoid running afoul of the First and Fourteenth Amendments and to ensure consumers may receive information about the impacts of an opt out request as they engage in the opt out process with a business.

III. The Proposed Modifications Should Impose the Same Notice Requirements on Authorized Agents as They Impose on Businesses

The proposed modifications to the CCPA regulations would require a business to ask an authorized agent for proof that a consumer gave the agent signed permission to submit a rights request.¹⁵ Although this provision helps ensure businesses can take steps to verify that authorized agents are acting on the true expressed wishes of consumers, the proposed modifications do not offer consumers sufficient protections from potential deception by authorized agents. For example, while the proposed modifications would impose additional notice obligations on businesses,¹⁶ those requirements do not extend to authorized agents. Authorized agents consequently have little to no guidelines or rules they must follow with respect to their communications with consumers, while businesses are subject to onerous, highly restrictive requirements regarding the mode and content of the information they may provide to Californians. The asymmetry between the substantial disclosure obligations for businesses and the lack thereof for authorized agents could enable (and, in fact, could incentivize) some agents to give consumers misleading

¹² *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980).

¹³ *Id.*

¹⁴ *Sorrell v. IMS Health Inc.*, 564 U.S. 572, 565 (2011).

¹⁵ Cal. Code Regs. tit. 11, § 999.326(a) (proposed Oct. 12, 2020).

¹⁶ *Id.* at § 999.315(h)(3).

or incomplete information. We encourage the OAG to take steps to modify the proposed modifications to the CCPA regulations in order to equalize the notice requirements placed on businesses and agents, thus ensuring consumers can act on an informed basis under CCPA. In Section II of this submission, we discuss related First Amendment and communications fairness issues implicit in a balanced consumer privacy notice regime.

IV. Proposed Modifications to the CCPA Regulations Should Enable Flexibility in Methods of Providing Offline Notice

The proposed modifications to the CCPA regulations related to offline notices present a number of problems for consumers and businesses. As written, the CCPA implementing regulations already provide sufficient guidance to businesses regarding the provision of offline notice at the point of personal information collection in brick-and-mortar stores.¹⁷ The proposed modifications are more restrictive and prescriptive than the current plain text of the CCPA regulations, would restrict businesses' speech, would remove the flexibility businesses need to effectively communicate information to their customers, and would unnecessarily impede business-consumer interactions. We therefore ask the OAG to update the proposed modifications to: (1) remove the proposed illustrative example associated with brick-and-mortar stores, and (2) explicitly enable businesses communicating with Californians by phone to direct them to an online notice where CCPA-required disclosures are made to satisfy their offline notice obligation, a medium which is more familiar to consumers for these sorts of disclosures along with having the added benefit of being able to present additional choices to the consumer.

The proposed modifications would require businesses that collect personal information when interacting with consumers offline to "provide notice by an offline method that facilitates consumers' awareness of their right to opt-out."¹⁸ The proposed modifications proceed to offer the following "illustrative examples" of ways businesses may provide such notice: through signage in an area where the personal information is collected or on the paper forms that collect personal information in a brick-and-mortar store, and by reading the notice orally when personal information is collected over the phone.¹⁹ While the illustrative examples set forth limited ways businesses can give notice in compliance with the CCPA, they are more restrictive than existing provisions of the CCPA regulations and detract from the flexibility businesses need to provide required notices that do not burden consumers or cause unreasonable friction or frustration during the consumer's interaction with the business.

The illustrative example related to brick-and-mortar store notification sets forth redundant methods by which businesses may provide notices in offline contexts. The CCPA regulations already address such methods of providing offline notice at the point of personal information collection by stating, "[w]hen a business collects... personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online."²⁰ The proposed modifications regarding notice of the right to opt out in offline contexts are therefore unnecessary, as the regulations already address the very same methods of providing offline notice and offer sufficient clarity and flexibility to businesses in providing such notice.

In addition, the proposed modifications related to brick-and-mortar store notification are overly prescriptive. They include specific requirements about the *proximity* of the offline notice to the area where personal information is collected in a store. The specificity of these illustrative examples could result in

¹⁷ Cal. Code Regs. tit. 11, § 999.305(a)(3)(c).

¹⁸ Cal. Code Regs. tit. 11, § 999.306(b)(3) (proposed Oct. 12, 2020).

¹⁹ *Id.*

²⁰ Cal. Code Regs. tit. 11, § 999.305(a)(3)(c).

over-notification throughout a store as well as significant costs. For example, the proposed modification could be interpreted to require signage at each cash register in a grocery store, as well as signage at the customer service desk, in the bakery area of the store where consumers can submit requests for cake deliveries, and in any other location where personal information may be collected. They also do not account for different contexts of business interactions with consumers. A business operating a food truck, for instance, would have different offline notice capabilities than an apparel store. A single displayed sign in a brick-and-mortar store, or providing a paper version of notice, would in most instances provide sufficient notice to consumers of their right to opt out under the CCPA. Bombarding consumers with physical signs at every potential point of personal information collection could be overwhelming and would ultimately not provide consumers with more awareness of their privacy rights. In fact, this strategy is more likely to create privacy notice fatigue than any meaningful increase in privacy control, thus undercutting the very goals of the CCPA.

Additionally, the proposed modifications' illustrative example of providing notice orally to consumers on the phone appears to suggest that reading the full notice aloud is the only way businesses can provide CCPA-compliant notices via telephone conversations. Reading such notice aloud to consumers would unreasonably burden the consumer's ability to interact efficiently with a business customer service representative and would likely result in consumer annoyance and frustration. Requiring businesses to keep consumers on the phone for longer than needed to address the purpose for which the consumer contacted the business would introduce unneeded friction into business-consumer relations. Instead, businesses should be permitted to direct a consumer to an online link where information about the right to opt out is posted rather than provide an oral catalog of information associated with particular individual rights under the CCPA.

The proposed modifications' addition of illustrative examples regarding methods of offline notice is unnecessary, redundant, and inflexible. These modifications would result in consumer confusion, leave businesses wondering if they may take other approaches to offline notices, and if so, how they may provide such notice within the strictures of the CCPA. We therefore ask the OAG to remove the proposed illustrative example associated with brick-and mortar stores as well as clarify that businesses communicating with consumers via telephone may direct them to an online website containing the required opt out notice as an acceptable way of communicating the right to opt out.

* * *

Thank you for the opportunity to submit input on the content of the proposed modifications to the CCPA regulations. Please contact Mike Signorelli of Venable LLP at [REDACTED] with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Lou Mastria
Executive Director
Digital Advertising Alliance

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

Clark Rector
Executive VP-Government Affairs
American Advertising Federation



December 27, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Fourth Set of Proposed Modifications to Text of California Consumer Privacy Act Regulations

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the fourth set of proposed modifications to the text of the California Consumer Privacy Act ("CCPA") regulations.¹

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising expenditures. Locally, our members are estimated to help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.²

For more than a year, our members have been communicating with consumers about their CCPA rights and how to effectuate them. As a result, our members have experience in operating under the CCPA and interacting with consumers. We have learned valuable insights about how to support consumer privacy rights under this new legal regime, including that operational flexibility is vital.

Not all interactions with consumers are the same nor are all business operations. There is no "one-size fits all" approach to the CCPA. We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous comment submissions and in this letter, the draft regulations implementing the CCPA should be updated to provide greater clarity, better enable consumers to exercise informed choices, and help businesses in their efforts to continue to provide value to Californians and support the state's economy.³

¹ See California Department of Justice, *Notice of Fourth Set of Proposed Modifications to Text of Regulations and Addition of Documents and Information to Rulemaking File* (Dec. 10, 2020), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-4th-set-mods.pdf>.

² IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <http://www.ana.net/getfile/23045>.

³ Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG's proposed rules implementing the CCPA. See *Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA 00000431 - 00000442; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-15day-comments-set1.pdf> at CCPA 15DAY_000554 - 000559; *Second Set of Proposed Regulations Implementing the California Consumer Privacy Act*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA 2ND15DAY_00309 - 00313; *Third Set of Proposed Regulations Implementing the California Consumer*

Companies and consumers have been adapting to the “Do Not Sell My Personal Information” tagline for more than a year. This effort has included refashioning digital properties, as well as instituting backend processes to meet the compliance requirements of the CCPA even as a new ballot initiative, the California Privacy Rights Act (or “Proposition 24”), was moving forward. These most recent proposed modifications by the OAG to the CCPA regulations set forth ambiguous terms surrounding a proposed online button almost a full year after the law went into effect. Among other things, this round of modifications fails to clarify whether the button is optional or mandatory. The proposed changes also do not leave room for the deployment of alternative icons, such as the CCPA Privacy Rights Icon in market provided by the Digital Advertising Alliance (“DAA”),⁴ or other methods, such as a text only link in applicable scenarios, to facilitate consumers’ right to opt out of personal information sales. The OAG should reconsider these provisions, or at the very least clarify them so businesses can take steps to comply with the new terms as soon as possible.

Additionally, changes the OAG made during the third set of proposed modifications to the CCPA regulations set forth a prescriptive interpretation of the law that could limit businesses’ ability to support employment in California and the state’s economy during these unprecedented times. We reassert the issues we previously raised with those provisions in this submission. As explained in more detail in the sections that follow below, the OAG’s potential changes to Section 999.315 would inhibit consumers from receiving transparent information and impinge on businesses’ right to free speech. In addition, the proposed modifications to Section 999.326 would not provide any protections for consumers related to their communications with authorized agents, as such agents are not presently held to similar consumer notice rules as businesses. Finally, the OAG’s proposed edits to Section 999.306 regarding offline notice of the right to opt out could stymie the flexibility businesses need to provide effective offline notices to consumers. We consequently ask the OAG to strike or modify these changes per the below comments.

Our members are committed to offering consumers robust privacy protections while simultaneously providing them with access to ad-funded news, apps, and a host of additional online services. These are offerings we have all become much more dependent on in recent months with the widespread proliferation of the COVID-19 pandemic. Ad-supported online content and services have been available to consumers and will continue to be available to consumers so long as laws allow for innovation and flexibility without unnecessarily tilting the playing field away from the ad-subsidized model. We believe a regulatory scheme that offers strong individual privacy protections and enables continued economic advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA regulations for Californians as well as protect the economy.

I. The Regulations Should Clarify That the Proposed New Button is Discretionary and Not Preclude Use of Other Icons Presented in Conjunction with the Text Link

In the fourth set of proposed modifications to the CCPA regulations, the OAG reinserted terms setting forth a specific graphic for a button enabling consumers to opt out of personal information sales. The proposed modifications state that the proposed button “*may* be used” in addition to posting a notice of the right to opt-out online, but not in lieu of such notice or the “Do Not Sell My Personal Information” link.⁵ In the very next subsection, the proposed rules state that when a business provides a “Do Not Sell My Personal Information” link, the proposed button “*shall* be added to the left” of the link.⁶ The language describing the proposed button is thus unclear, as it does not adequately explain whether providing the

Privacy Act, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-written-comm-3rd-15-day-period.pdf> at CCPA_3RD15DAY_00111 - 00118.

⁴ DAA, *Opt Out Tools*, located at <https://www.privacyrights.info/>.

⁵ Cal. Code Regs. tit. 11, § 999.306(f)(1) (proposed Dec. 10, 2020) (emphasis added).

⁶ *Id.* at § 999.306(f)(2) (emphasis added).

button is discretionary or mandatory for businesses that sell personal information. We ask the OAG to confirm that the proposed button is discretionary as well as to provide flexibility for businesses to use alternative, industry-developed icons that signal the right to opt out of personal information sales to California consumers.

As the founding members of the DAA YourAdChoices program and corresponding icon,⁷ we understand the benefits a widely recognizable icon can bring to provide transparency and choices to consumers. In fact, in November 2019, the DAA announced its creation of a tool and corresponding Privacy Rights Icon to provide consumers with a clear and recognizable mechanism to opt out of personal information sales under the CCPA.⁸ Icons and corresponding privacy programs created by the DAA have a history of success. The YourAdChoices icon has been served globally at a rate of more than one trillion times per month, and its recognition continues to grow. In a 2016 survey, more than three in five respondents (61 percent) recognized the YourAdChoices icon at least a little, and half (50 percent) said they recognized it a lot or somewhat. For the CCPA, there is a need for flexibility in how this novel law is implemented in the market. The OAG should allow the marketplace to determine the best opt-out button approach, including allowing the option for use of an icon promulgated in relation to industry-driven opt-out mechanisms, rather than creating uncertainty by mandating a new graphic that businesses must use.

Moreover, adding the button as a requirement now, nearly a year after the CCPA became effective and more than five months after the OAG began enforcing the law, would create unnecessary new compliance costs for businesses to reconfigure websites and consumer-facing properties after they have already taken significant steps to update their practices per the CCPA's requirements. We therefore ask the OAG to clarify that the new opt-out button is discretionary rather than mandatory, and businesses that provide a "Do Not Sell My Personal Information" link are not required to also provide the proposed button. We also ask the OAG to provide flexibility for businesses to utilize other icons to signal a consumer's right to opt out of personal information sales, such as the DAA's CCPA Privacy Rights Icon. The OAG should reconsider the need to create new iconography and should instead partner with industry on the already existing DAA Privacy Rights Icon to help lead consumers to choices about how their personal information is used and shared.

II. The Regulations Should Support Consumers' Awareness of the Implications of Their Privacy Decisions, Not Hinder It in Violation of the First Amendment

The proposed online and offline modifications unreasonably limit consumers' ability to access accurate and informative disclosures about business practices as they engage in the opt out process. Ultimately, this restriction on speech would not benefit consumers or advance a substantial interest. The proposed rules state: "Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request."⁹ This language unduly limits consumers from receiving important information as they submit opt out requests. It is also overly limiting in the way that businesses may communicate with consumers. As highlighted above, data-driven advertising provides consumers with immensely valuable digital content for free or low-cost, as well as critical revenue for publishers, by increasing the value of ads served to consumers. As the research cited above also confirms, consumers have continually expressed their preference for ad-supported digital content and services, rather than having to pay significant fees for a wide range of apps, websites, and internet services they use. However, as a result of the proposed modifications, consumers' receipt of factual, critical information about the nature of the ad-supported

⁷ Digital Advertising Alliance, *YourAdChoices*, located at <https://youradchoices.com/>.

⁸ DAA, *Digital Advertising Alliance Announces CCPA Tools for Ad Industry* (Nov. 25, 2019), located at <https://digitaladvertisingalliance.org/press-release/digital-advertising-alliance-announces-ccpa-tools-ad-industry>.

⁹ Cal. Code Regs. tit 11, § 999.315(h)(3) (proposed Oct. 12, 2020).

Internet would be unduly hindered, thereby undermining a consumer's ability to make an informed decision. A business should be able to effectively communicate with consumers to inform them about how and why their data is used, and the benefit that data-driven advertising provides as a critical source of revenue.

It is no secret that consumers greatly value the information they can freely access online from digital publishers. However, local news publishers, for instance, continue to struggle to get readers to pay subscription fees for their content, even though this content is highly valuable to consumers and society. Thus, most news publishers have become increasingly reliant on tailored advertising, because it provides greater revenue than traditional advertising.¹⁰ However, the proposed modifications, as drafted, could obstruct consumers from receiving truthful, important information by hindering a business' provision of a reasonable notice to consumers about the funding challenges opt outs pose to their business model.

The CCPA regulations should not prevent consumers from receiving and businesses from providing full, fair, and accurate information during the opt out process. The proposed modification would impede consumers from receiving important information about their privacy choices, such as information about the vital nature of the ad-supported Internet, and, as explained in Section III, they may be contemporaneously receiving partial or misleading negative information about their opt out rights.

To ensure a fully informed privacy choice, consumers must have every ability to access information about business practices and the benefits of the digital advertising ecosystem. Providing ample and timely opportunities for consumers to gain knowledge about their choice to opt out is of paramount importance to avoid confusion and ignorance; this allows a consumer to be fully informed about the actual implications of their decision. By prohibiting a business from requiring a consumer "to click through or listen to reasons why they should not submit a request to opt-out *before* confirming their request" the regulations do not safeguard against this concern. As presently written, the proposed modification appears to limit businesses' ability to provide such vital information as a consumer is opting out, even if such information is presented in a seamless way. It is unclear what amount of information, or what method in which such information is presented, could constitute a violation of the rules. Instead of setting forth prohibitive rules that could reduce the amount of information and transparency available to consumers online, the OAG should prioritize facilitating accurate and educational exchanges of information from businesses to consumers. As a result, we ask the OAG to revise the text of the proposed modification in Section 999.315(h)(3) so that businesses are permitted to describe the impacts of an opt-out choice while facilitating the consumer's request to opt out.

Additionally, the restrictions created by this proposed modification infringe on businesses' First and Fourteenth Amendment right to commercial speech. As written, Section 999.315(h)(3) restricts the information consumers can receive from businesses as they submit opt out requests by limiting the provision of accurate and truthful information to consumers. The Supreme Court has explained that "people will perceive their own best interest if only they are well enough informed, and . . . the best means to that end is to open the channels of communication, rather than to close them. . . ."¹¹ Because this proposed regulation prescriptively regulates channels of communication, it violates the First and Fourteenth Amendments.

The state may not suppress speech that is "neither misleading nor related to unlawful activity" unless it has a substantial interest in restricting this speech, the regulation directly advances that interest,

¹⁰ DAA, *Study: Online Ad Value Spikes When Data Is Used to Boost Relevance* (Feb. 10, 2014), located at <https://digitaladvertisingalliance.org/press-release/study-online-ad-value-spikes-when-data-used-boost-relevance>.

¹¹ *Virginia Pharmacy Board v. Virginia Citizens Consumer Council*, 425 U. S. 748, 770 (1976).

and the regulation is narrowly tailored to serve that interest.¹² The proposed regulation fails each part of the test:

- **No substantial interest:** Although there is no stated justification in the proposal, the most likely interest would be to streamline opt out requests by making it easier and faster to submit opt-outs. The OAG presumably wants nothing to impede consumers from opting out, but it is unclear because the OAG has not affirmatively stated its purpose for the proposed modification. Consumers should be made aware of the ramifications of their opt out decisions as they are opting out – not after confirming a request – so they do not make opt out choices to their detriment because they do not know the effect of such choices. For this reason, they should be able to receive information from businesses about the consequences of their opt out choices as they are submitting opt out requests. Providing information concerning the impact of an opt out is not an impediment to the process, but rather improves it.
- **No advancement of the interest:** If streamlining opt out requests to remove perceived impediments is the justification for the proposed rule, then the proposal does not advance that interest. The proposed regulation already includes many other specific requirements that facilitate speed and ease of opt-outs, including a requirement to use the minimal number of steps for opt-outs (and no more than the number of steps needed to opt in), prohibiting confusing wording, restricting the information collected, and prohibiting hiding the opt-out in a longer policy, all of which directly advance this interest without suppressing speech. The proposed rule limiting businesses from clicking through or listening to reasons would not make the opt out process easier for consumers, because it could result in consumers making uninformed choices if they are not notified of the consequences of their decision to opt out as they are making it. A “regulation may not be sustained if it provides only ineffective or remote support for the government’s purpose.”¹³ This proposed regulation is both ineffective and provides no support for the government’s purpose.
- **Not narrowly tailored:** The proposed regulation is an overly broad and prescriptive restriction on speech that hinders accurate and educational communications to consumers about the consequences of a decision to opt-out. The regulations already include various other provisions that work to streamline the opt out process. “[I]f the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.”¹⁴ As noted above, there are many ways to craft regulations to require simple and fast opt-out mechanisms that do not suppress lawful and truthful speech.

In sum, the regulation violates each and every prong of the framework for evaluating commercial speech. “As in other contexts, these standards ensure not only that the state’s interests are proportional to the resulting burdens placed on speech but also that the law does not seek to suppress a disfavored message.”¹⁵ The proposed regulation would do exactly that. Thus, it is a content-based restriction on speech, subject to heightened scrutiny. The U.S. Supreme Court has made clear that the burden is on the government to justify content-based restrictions on lawful speech, and the failure to even state a basis for this restriction fails to meet this requirement.¹⁶ The OAG should revise the text of the proposed

¹² *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980); *see also Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).

¹³ *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980).

¹⁴ *Id.*

¹⁵ *Sorrell v. IMS Health Inc.*, 564 U.S. 572, 565 (2011).

¹⁶ *E.g., Reed v. Town of Gilbert*, 576 U.S. 155, 171 (2015) (citing *Arizona Free Enter. Club’s Freedom Club PAC v. Bennett*, 564 U.S. 721 (2011)).

modification in Section 999.315(h)(3) to avoid running afoul of the First and Fourteenth Amendments and to ensure consumers may receive information about the impacts of an opt out request as they engage in the opt out process with a business.

III. The Proposed Modifications Should Impose the Same Notice Requirements on Authorized Agents as They Impose on Businesses

The proposed modifications to the CCPA regulations would require a business to ask an authorized agent for proof that a consumer gave the agent signed permission to submit a rights request.¹⁷ Although this provision helps ensure businesses can take steps to verify that authorized agents are acting on the true expressed wishes of consumers, the proposed modifications do not offer consumers sufficient protections from potential deception by authorized agents. For example, while the proposed modifications would impose additional notice obligations on businesses,¹⁸ those requirements do not extend to authorized agents. Authorized agents consequently have little to no guidelines or rules they must follow with respect to their communications with consumers, while businesses are subject to onerous, highly restrictive requirements regarding the mode and content of the information they may provide to Californians. The asymmetry between the substantial disclosure obligations for businesses and the lack thereof for authorized agents could enable some agents to give consumers misleading or incomplete information. We encourage the OAG to take steps to modify the proposed modifications to the CCPA regulations in order to equalize the notice requirements placed on businesses and agents, thus ensuring consumers can act on an informed basis under CCPA. In Section II of this submission, we discuss related First Amendment and communications fairness issues implicit in a balanced consumer privacy notice regime.

IV. Proposed Modifications to the CCPA Regulations Should Enable Flexibility in Methods of Providing Offline Notice

The proposed modifications to the CCPA regulations related to offline notices present a number of problems for consumers and businesses. As written, the CCPA implementing regulations already provide sufficient guidance to businesses regarding the provision of offline notice at the point of personal information collection in brick-and-mortar stores.¹⁹ The proposed modifications are more restrictive and prescriptive than the current plain text of the CCPA regulations, would restrict businesses' speech, would remove the flexibility businesses need to effectively communicate information to their customers, and would unnecessarily impede business-consumer interactions. We therefore ask the OAG to update the proposed modifications to: (1) remove the proposed illustrative example associated with brick-and-mortar stores, and (2) explicitly enable businesses communicating with Californians by phone to direct them to an online notice where CCPA-required disclosures are made to satisfy their offline notice obligation, a medium which is more familiar to consumers for these sorts of disclosures along with having the added benefit of being able to present additional choices to the consumer. This sort of operational flexibility is necessary for businesses to convey important notices in context.

The proposed modifications would require businesses that sell personal information to “inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request” when interacting with consumers offline.²⁰ The proposed modifications proceed to offer the following “illustrative examples” of ways businesses may provide such notice: through signage in an area where the personal information is collected or on the paper forms that collect personal information in a

¹⁷ Cal. Code Regs. tit. 11, § 999.326(a) (proposed Oct. 12, 2020).

¹⁸ *Id.* at § 999.315(h)(3).

¹⁹ Cal. Code Regs. tit. 11, § 999.305(a)(3)(c) (finalized Aug. 14, 2020).

²⁰ Cal. Code Regs. tit. 11, § 999.306(b)(3) (proposed Dec. 10, 2020).

brick-and-mortar store, and by reading the notice orally when personal information is collected over the phone.²¹ While the illustrative examples set forth limited ways businesses can give notice in compliance with the CCPA, they are more restrictive than existing provisions of the CCPA regulations and detract from the flexibility businesses need to provide required notices that do not burden consumers or cause unreasonable friction or frustration during the consumer's interaction with the business.

The illustrative example related to brick-and-mortar store notification sets forth redundant methods by which businesses may provide notices in offline contexts. The CCPA regulations already address such methods of providing offline notice at the point of personal information collection by stating, “[w]hen a business collects... personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.”²² The proposed modifications regarding notice of the right to opt out in offline contexts are therefore unnecessary, as the regulations already address the very same methods of providing offline notice and offer sufficient clarity and flexibility to businesses in providing such notice.

In addition, the proposed modifications related to brick-and-mortar store notification are overly prescriptive. They include specific requirements about the *proximity* of the offline notice to the area where personal information is collected in a store. The specificity of these illustrative examples could result in over-notification throughout a store as well as significant costs. For example, the proposed modification could be interpreted to require signage at each cash register in a grocery store, as well as signage at the customer service desk, in the bakery area of the store where consumers can submit requests for cake deliveries, and in any other location where personal information may be collected. They also do not account for different contexts of business interactions with consumers. A business operating a food truck, for instance, would have different offline notice capabilities than an apparel store. A single displayed sign in a brick-and-mortar store, or providing a paper version of notice, would in most instances provide sufficient notice to consumers of their right to opt out under the CCPA. Bombarding consumers with physical signs at every potential point of personal information collection could be overwhelming and would ultimately not provide consumers with more awareness of their privacy rights. In fact, this strategy is more likely to create privacy notice fatigue than any meaningful increase in privacy control, thus undercutting the very goals of the CCPA.

Additionally, the proposed modifications' illustrative example of providing notice orally to consumers on the phone appears to suggest that reading the full notice aloud is the only way businesses can provide CCPA-compliant notices via telephone conversations. Reading such notice aloud to consumers would unreasonably burden the consumer's ability to interact efficiently with a business customer service representative and would likely result in consumer annoyance and frustration. Requiring businesses to keep consumers on the phone for longer than needed to address the purpose for which the consumer contacted the business would introduce unneeded friction into business-consumer relations. Instead, businesses should be permitted to direct a consumer to an online link where information about the right to opt out is posted rather than provide an oral catalog of information associated with particular individual rights under the CCPA.

The proposed modifications' addition of illustrative examples regarding methods of offline notice is unnecessary, redundant, inflexible, and likely highly costly for many businesses. These modifications would result in consumer confusion, leave businesses wondering if they may take other approaches to offline notices, and if so, how they may provide such notice within the strictures of the CCPA. We therefore ask the OAG to remove the proposed illustrative example associated with brick-and mortar stores

²¹ *Id.*

²² Cal. Code Regs. tit. 11, § 999.305(a)(3)(c) (finalized Aug. 14, 2020).

as well as clarify that businesses communicating with consumers via telephone may direct them to an online website containing the required opt out notice as an acceptable way of communicating the right to opt out.

* * *

Thank you for the opportunity to submit input on the content of the proposed modifications to the CCPA regulations. Please contact Mike Signorelli of Venable LLP at [REDACTED] with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

Lou Mastria
Executive Director
Digital Advertising Alliance



July 28, 2021

California Office of the Attorney General
Attorney General Rob Bonta
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Response to CCPA FAQ Regarding User-Enabled Controls and Related Enforcement Letters

Dear Attorney General Bonta:

The undersigned trade associations and organizations collectively represent a broad cross-section of the Californian and United States business community spanning various industries including advertising and marketing, analytics, magazine publishing, Internet and online services, financial services, package delivery, cable and telecommunications, transportation, retail, real estate, insurance, entertainment, auto, and others. Our organizations have a long history of supporting consumers' ability to exercise choice over uses of data for digital advertising. Enabling consumers to express their preferences and exercise control through easy-to-use, user-enabled choice mechanisms is a foundational aspect of data privacy that we have championed for decades. However, we are concerned that the OAG's new FAQ response regarding user-enabled global privacy controls will cause confusion for consumers and businesses, rather than effectuating genuine user choices.

In particular, we maintain the following three concerns. First, the FAQ mandate directly conflicts with the approach taken in the California Privacy Rights Act of 2020 ("CPRA"), which becomes operative in less than 18 months. Second, there was no public process for evaluating or

considering the cited tools or the particular implementations by the browser referenced in the FAQ, and as a result there are diverging perspectives around what constitutes a tool that is “user enabled.” Finally, the existence of the FAQ unnecessarily prejudices a subject matter on which the California Privacy Protection Agency (“CPPA”) is directed by law to promulgate rules. These concerns are compounded by the recent publicly-reported enforcement letters sent by the OAG to companies on adherence to such signals.¹ We therefore ask you to retract this FAQ response, reconsider your enforcement approach to user-enabled global privacy controls, and defer to California’s new privacy agency on the subject.

- **The FAQ response conflicts with the approach taken in the CPRA. This will lead to confusion for consumers and businesses.** Not only does the California Consumer Privacy Act of 2018 (“CCPA”) not direct the Attorney General to create and mandate adherence to the controls described in Section 999.315(c) of the regulations implementing the law,² but the FAQ response stands in direct contrast to the approach to such controls taken in the CPRA. According to the CPRA, businesses “may elect” to either (a) “[p]rovide a clear and conspicuous link on the business’s internet homepage(s) titled ‘Do Not Sell or Share My Personal Information’” **or** (b) allow consumers to “opt-out of the sale or sharing of their personal information... through an opt-out preference signal sent with the consumer’s consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]”³ Despite this choice that will become available to businesses in a short time, the FAQ response and decision to send enforcement letters to businesses regarding user-enabled privacy controls that do not align with the CPRA is unnecessary and creates confusion in the market. The OAG consequently takes a position on such controls that does not reflect California law and is likely to be different from the approach spelled out by new regulations implementing the CPRA. This will result in confusion for consumers and businesses.
- **The FAQ statement directly conflicts with the CPRA mandate explicitly directing California’s new privacy agency to issue specific rules governing user-enabled global privacy controls.** The CPRA tasks the CPPA to issue particularized regulations governing user-enabled global privacy controls to help ensure consumers and businesses are protected from intermediary interference. Given the lack of formal process employed with respect to the OAG’s proposed application of global privacy controls and the FAQ response, it does not appear that these safeguards have been considered and addressed. For example, the CPRA instructs the CPPA to “ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal *cannot unfairly disadvantage another business.*”⁴ According to the CPRA, the CPPA must also ensure user-enabled global privacy controls “*clearly*

¹ See *State of California Department of Justice, Rob Bonta Attorney General, California Consumer Privacy Act (CCPA) FAQ Section B, #7 and #8*, available at <https://oag.ca.gov/privacy/ccpa>; see also Kate Kaye, *California’s attorney general backs call for Global Privacy Control adoption with fresh enforcement letters to companies*, DIGIDAY (Jul. 16, 2021), available at <https://digiday.com/marketing/californias-attorney-general-backs-call-for-global-privacy-control-adoption-with-fresh-enforcement-letters-to-companies/>.

² Cal. Code Regs. tit. 11, § 999.315(c); see also Joint Ad Trades Comments on the Second Set of Proposed Regulations Implementing the CCPA at CCPA_2ND15DAY_00310 - 00313, available [here](#) (noting California Administrative Procedural Act and constitutional concerns with Section 999.315(c) of the regulations implementing the CCPA).

³ CPRA, Cal. Civ. Code § 1798.135(b)(3).

⁴ CPRA, Cal. Civ. Code § 1798.185(a)(19)(A) (emphasis added).

represent a consumer's intent and [are] free of defaults constraining or presupposing such intent.”⁵

In contrast, the OAG's FAQ response does not ensure that any of the safeguards set forth in the CPRA's regulatory instructions are followed. For instance, the OAG's FAQ response lists a browser that sends opt-out signals by default without consulting the consumer, and such signals are unconfigurable.⁶ The OAG's FAQ response therefore does not provide any means to enable businesses to determine whether a global privacy control signal, as implemented by particular browsers, is truly user-enabled, or if it is instead sent or communicated by an intermediary in the ecosystem without the consumer's consent. Moreover, the FAQ response contravenes the will of Californians, as expressed in passing the CPRA ballot initiative, that privacy regulation on the subject of user-enabled global privacy controls should come from the CPPA as opposed to the OAG.

- **New OAG guidance regarding user-enabled global privacy controls should be developed through a deliberative process that considers stakeholder input.** The OAG's FAQ response was posted to its website without any sort of formal deliberation or process prior to publication. Legal and material guidance such as those contained in the FAQ should only be issued after a carefully deliberated formal process that allows for public input. New rules or guidance regarding user-enabled global privacy controls should be afforded the benefit of a formal process, including public comment and thoughtful evaluation.

Such process should also indicate how the OAG and/or CPPA will (i) ensure such controls are compliant with the CPRA, (ii) monitor control providers to ensure their compliance with law and the standards set forth in the CPRA, and (iii) set forth a system to ensure that modifications by browsers and other intermediaries remain compliant with law to avoid circumstances where changes “unfairly disadvantage another business” or no longer “clearly represent a consumer's intent and [are] free of defaults constraining or presupposing such intent.” Issuing a rule on such controls without providing a deliberative process risks creating significant confusion and unworkable policy for consumers and businesses alike.

* * *

The undersigned trade associations and organizations fully support empowering consumer choice and advancing workable privacy protections for Californians. However, the position reflected in the OAG's recent FAQ response and enforcement letters was issued without formal process and contradicts the approach to user-enabled global privacy controls taken in the CPRA. We therefore respectfully ask you to reconsider the FAQ response, as well as your enforcement

⁵ *Id.*

⁶ See Brave, *Global Privacy Control, a new Privacy Standard Proposal*, now Available in Brave's Desktop and Android Testing Versions, available at <https://brave.com/global-privacy-control/> (“Importantly, Brave does not require users to change anything to start using the GPC to assert your privacy rights. For versions of Brave that have GPC implemented, the feature is on by default and unconfigurable.”)

approach concerning user-enabled global privacy controls, and to instead defer to the CPPA on the issue. Please contact Mike Signorelli of Venable LLP at [REDACTED] with questions on this letter.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
[REDACTED]

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
[REDACTED]

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
[REDACTED]

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[REDACTED]

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
[REDACTED]

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[REDACTED]

Howard Fienberg
Senior VP, Advocacy
Insights Association
[REDACTED]

Shoeb Mohammed
Policy Advocate
California Chamber of Commerce
[REDACTED]

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
[REDACTED]

Cameron Demetre
Executive Director, CA & the Southwest
TechNet
[REDACTED]

Anton van Seventer
State Privacy & Security Coalition
[REDACTED]

CC: California Privacy Protection Agency

EXHIBIT B

PRINCIPLES FOR USER-ENABLED CHOICE SETTING MECHANISM

A Choice Setting should meet the following criteria:

1. **Accessing the Setting.** A Choice Setting shall be activated in the settings panel of a browser and/or device, which is accessible from a menu. Additional prompts or other means of accessing a Choice Setting may be offered in addition to the setting panel, but such additional prompts or means should not unfairly disadvantage an entity.
2. **Describe Setting & Effect.** A Choice Setting shall communicate the following:
 - a. **Effect of Choice.** The effect of exercising such choice including that a Choice Setting signal is limited to communicating a preference to opt out from the sale of personal information, specific types of advertising, and/or any other legal right provided by law; and the fact that some data may still be collected and used for purposes not subject to the rights provided by law following the sending of a choice signal;
 - b. **Scope of Opt Out.** Choice made via the Choice Setting applies to the browser or device from which such choice is made, or for the consumer, if known to the entity receiving the signal and required by law; and
 - c. **Affirmative Direction to Sell.** The fact that if a consumer affirmatively allows a particular entity to collect, sell, or use personal information about interactions, viewing and/or activity from Web sites, devices, and/or applications, the activation of the Choice Setting will not limit that collection, sale, or use from such entity.
3. **Affirmative Step.** The consumer shall affirmatively consent to turn on or activate the Choice Setting via the settings panel of a browser and/or device. Such ChoiceSetting may not be preselected, turned on, or activated by default.
4. **Option to Withdraw Choice.** A Choice Setting shall provide a means for a consumer to turn off, deactivate, or revoke consent for the Choice Setting through the same means the consumer previously made the affirmative choice to turn on or activate the Choice Setting.
5. **Jurisdictional Signal.** The Choice Setting should indicate the jurisdiction(s) from which choice is made in a manner that the entity receiving the signal may determine the applicable legal requirement(s).

* * *

From: Peter Leroe-Muñoz [REDACTED]
Sent: 11/5/2021 10:39:10 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21, Silicon Valley Leadership Group Comments
Attachments: CPPA, Preliminary Comments.pdf

[EXTERNAL]: [REDACTED]

CAUTION: THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!
DO NOT: click links or open attachments unless you know the content is safe.
NEVER: provide credentials on websites via a clicked link in an Email.

Hello,

Please find attached Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21) from the Silicon Valley Leadership Group.

My thanks,
Peter

Peter Leroe-Muñoz

General Counsel
SVP, Tech & Innovation
[REDACTED] svlg.org

Connect with us: [Twitter](#) | [LinkedIn](#) | [Facebook](#)





Ahmad Thomas, CEO
Silicon Valley Leadership Group

Jed York, Chair
San Francisco 49ers

Eric S. Yuan, Vice Chair
Zoom Video Communications

James Gutierrez, Vice Chair
Luvu

Victoria Huff Eckert, Treasurer
PwC US

Greg Becker
Silicon Valley Bank

Anil Chakravarthy
Adobe Systems

Aart de Geus
Synopsys

Raquel Gonzalez
Bank of America

Vintage Foster
AMF Media Group

Paul A. King
Stanford Children's Health

Ibi Krukuboko
EY

Alan Lowe
Lumentum

Judy C. Miner
Foothill-De Anza
Community College District

Rao Mulpuri
View

Kim Polese
CrowdSmart

Ryan Popple
Proterra

Sharon Ryan
Bay Area News Group

Tom Werner
SunPower

November 5, 2021

California Privacy Protection Agency
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)**

Esteemed Agency Members:

I am writing on behalf of the Silicon Valley Leadership Group to provide preliminary comments on the proposed rulemaking under the California Privacy Rights Act of 2020. Our feedback is included in the attached Appendix A.

The Leadership Group was founded in 1978 by David Packard of Hewlett-Packard and represents more than 350 of Silicon Valley's most respected employers. Leadership Group member companies collectively provide nearly one of every three private sector jobs in Silicon Valley and we have a long history of supporting policies that promote innovation, stronger economic growth and improved transportation in California.

We are eager to work with your office to help clarify portions of the California Consumer Privacy Act, bring greater certainty to consumers and business about their respective rights and responsibilities and establish a framework that promotes both privacy and economic growth.

Sincerely,



Peter Leroe-Muñoz
General Counsel
SVP of Tech Policy



APPENDIX A

Preliminary Comments to the California Privacy Protection Agency

New use of personal information. Where a business has proactively and directly notified consumers that the business intends to use personal information in a new way, explicit consumer consent should not be required for such use.

Opt-out of sale of personal information. A business should be exempt from providing a notice of a right to opt-out when the business publishes a change in its Privacy Policy for a determined period of time to give consumers the right to opt-out.

Estimated value of data. Language referencing any estimated value of a consumer's data, as well as any description of the methodology for calculating such value, should be eliminated. Determining the value of any particular consumer's personal information is highly specific and time intensive. Moreover, any estimation would require significant speculation at the time of collection, rendering the calculation unreliable.

Non-conforming requests. If a consumer submits a request in a non-conforming method or manner, businesses should not attempt to treat the request as if it were properly submitted, nor should they be required to remedy any such request.

Response time should begin with verification of requests. The proposed requirement that business must respond to a request within 45 days of receipt should be amended to respond within 45 days of when the request was verified. This allows a business to properly verify requests, which may take an extended period of time through no fault of the business.

Clarify "reasonable security measures" to include the NIST Cybersecurity Framework. "Reasonable security measures" should be properly clarified to include the National Institute of Standards and Technology ("NIST") Cybersecurity Framework. The Framework outlines best practices to establish and monitor security standards across diverse industries. Good faith compliance with the NIST Cybersecurity Framework should create a safe harbor from legal or regulatory liability under the California Consumer Privacy Act and other state privacy laws and regulations.

Industry standard authentication to verify requests. Businesses should be able to use their industry's standard authentication methodology to verify consumer requests.