Computer & Communications Industry Association
Tech Advocacy Since 1972

Via Electronic Mail (regulations@cppa.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://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.
[2] A list of CCIA members is available at https://www.ccianet.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. <u>Audits Performed by the Agency</u>

[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, consisted 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 adoom@ccianet.org.

Sincerely,

Alyssa Doom
State Policy Director
Computer & Communications Industry Association