CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

November 8, 2021

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

Re. *Preliminary Comments by the Civil Justice Association of California on Proposed Rulemaking Under the California Privacy Rights Act of 2020*

Dear California Privacy Protection Agency Board:

The Civil Justice Association of California[1] appreciates the opportunity to provide preliminary comments to the California Privacy Protection Agency ("Agency") in advance of the formal rulemaking process under the California Privacy Rights Act of 2020 (CPRA).

Businesses are eager for clarifying regulations that will guide compliance with the California Consumer Privacy Act (CCPA) and the CPRA. Both sets of laws are complex and contain vague provisions, making compliance difficult and creating liability exposure for good actors attempting to comply. The preliminary comments below provide guidance on important clarifications that will facilitate compliance by businesses and help to avoid unnecessary enforcements and litigation which is costly for both the state and businesses.

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

In general, the Agency should incorporate the following overarching principles into regulations for cybersecurity audits and risk assessments across all the identified topic areas. We spell out topic-specific guidance under the corresponding headings below.

- **Uniformity with global, federal, and other states' standards.** To avoid unnecessary complexity and burden for businesses and to promote interoperability, California should not be an outlier with respect to cyber security audits and risk assessments. These standards should be uniform across state lines conform with federal laws and regulations and Global Data Privacy Regulations (GDPR).[2]

[1] CJAC is a more than 40-year-old nonprofit organization representing a broad and diverse array of businesses and professional associations. A trusted source of expertise in legal reform and advocacy, we confront legislation, laws, and regulations that create unfair burdens on California businesses, employees, and communities.
[2] Global Data Privacy Regulations, https://gdpr-info.eu/

Additionally, to comply with CPRA, businesses should be allowed to use assessment processes that are generally accepted as best industry practice or by regulatory bodies, such as ISO 27000, NIST Cybersecurity Framework, Payment Card Industry Data Security Standard, Service Organization Control audits, and consent decrees with regulators like the Federal Trade Commission.

The Agency should accept audits and assessments performed under the foregoing standards and otherwise provide consistent regulations. Rules should also recognize that a single risk assessment may address a comparable set of processing operations that include similar activities.

- **Uniformity with existing California law and regulations.** In promulgating regulations, the Agency should also ensure consistency with existing California's laws and regulations impacting a variety of industries on matters of data security. For example, CPRA regulations should recognize with California's existing data security requirements under California Code of Civil Procedure section 1798.81.5.

- **Exempt applicant, employee, and independent contractor information.** The Agency should recognize permanent exceptions for processing personal information of job applicants, employees, and independent contractors collected and used solely in the context those roles. Regular audits or risk assessments requirements would create confusion and conflict with existing state and federal requirements applying to workers and create undue burden for businesses. This is consistent with the purpose and intent language of CPRA, which states that its implementation should "tak[e] into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses."[3]

- **Exempt trade secrets and confidential information.** The agency's regulation of audits and risk assessments should not require businesses to divulge trade secrets or other confidential information; redaction should be allowed. The transparency goal of CPRA would be frustrated if businesses lack assurance that compliance with documentation and disclosure requirements will not be used against them in future litigation. Moreover, audit and assessment information submitted to the Agency should be exempt from public inspection and copying under the California Public Records Act and be deemed not to constitute a waiver of any attorney-client privilege or work product protection.

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

- **Audits and assessment should provide flexibility.** Businesses need reasonable standards and flexibility under the new regulations to determine what is considered a significant risk to consumers based on the business' product or service and business' size and scope. Standards should also allow businesses to

[3] Proposition 24, CPRA, Section 3(A)(8).

continue to innovate and develop data protection technologies to further assess cybersecurity risks.

- **Significant risk should be tied to the likelihood of significant harm.** Regulations should define processing that has significant risk to consumers to mean processing of personal consumer information that, if compromised, is likely to create actual harm to a consumer or lead to unfavorable legal implications. Examples of real harm include identify theft or fraud, extortion, or physical injury from disclosure of sensitive personal information. Legal implications can include the sharing of information that could negatively impact decisions on employment, housing or other areas protected from discrimination under the law.

- **Data processed for fraud prevention or security purposes should be excluded.** Personal information processed for the benefit of fraud prevention, anti-money laundering processes, or to otherwise comply with existing legal obligations should be exempted from the definition of processing that presents a "significant risk to customers" as these activities protect consumers' privacy and security.

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."

- **Scope of audits should be risk-based.** Requirements for audit scope should focus on whether businesses have implemented and followed policies and procedures that secure personal information that is highest risk for the consumer's privacy or security.

- **Flexibility should be given to businesses on choice of auditor.** Businesses should have the flexibility to select qualified, independent third-party auditors to conduct assessments of their choice. Businesses should also have the option to self-audit if conducted in a manner consistent with existing laws and appropriate industry standards. A blanket mandate to use third-party auditors could result in significant burden and expense for businesses, with no added consumer benefit. Self-audits should be permitted.

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.

- **Scope of risk assessment should be limited to high-risk processing.** The Agency's regulations should balance the potential burden and expense of extensive audit requirements against consumer benefit to minimize the burden on business and maximize the value to consumers, including consideration of the following factors.
    - Technical and organizational measures and safeguards implemented by the business to mitigate privacy and security risks;
    - Reasonable expectations of consumers; and
    - The context of the processing with respect to business/consumer relationship.

- **Timing of audits should be tied to material changes or agency inquiries.** The regulations should require assessments to be performed only when a data processing practice is new or has materially changed in a way that poses new or increased consumer risk, or if there is an Agency investigation or inquiry. Requiring businesses to frequently or regularly conduct or submit risk assessments for the sake of routine could deluge the agency with submissions and will result in needless cost and operational burden, particularly for small and medium businesses.

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.

- **Risk-benefit analysis should consider context and other factors.** The determination of when risks to consumer privacy outweigh benefits of processing information should be a reasonableness standard that considers criteria such as.
    - Size and scope of the organization and nature, purpose and needs of the business.
    - Interruptions or other negative impacts on provision of goods and services to consumers without the processing.
    - Whether processing poses a heightened or substantial risk of harm to the consumer. Examples include monetization of data that directly identifies consumers, processing of sensitive data for secondary purposes, and the use of personal data that has legal implications.
    - Whether safeguards can mitigate risks for harm presented by processing.

- **Benefits of personal information collection in the context of employment or independent contractor relationships outweigh risks.** As noted above, when personal information is collected and used solely within the context of an individuals' role or former role as a job applicant, employee, or independent contractor, the regulations should recognize that the risk does not outweigh the benefit.

2. Automated Decisionmaking

In general, the Agency should incorporate the following overarching principles into regulations for automated decisionmaking (ADM) and profiling across all the identified topic areas. We spell out topic-specific guidance under the corresponding headings below.

- **Uniformity with existing global, federal, and state law and regulations.** In promulgating ADM regulations, the Agency should ensure consistency with existing global, federal and California laws and regulations governing ADM technology. For example, GDPR provides the right not to be subject to solely ADM decisions that have legal or significant impacts[4] and several states follow a similar approach. Also, the Fair Credit Reporting Act already requires entities to

[4] GDPR, Art. 22(1).

give adverse action notices when making a negative decision based on a credit report.

- **Focus regulations on ADM technology that impacts individual consumers.** Innovative ADM technologies are often used and can greatly facilitate general business operation and function, so ADM regulations should focus on technologies that impact individuals rather those geared to helping businesses to run efficiently and smoothly.

- **Consumers access to information should only be when there is a high-risk, final decision.** Consumers access to information about a business's use of ADM technology should only take place when there have been high-risk, final decisions that are fully automated, with no human participation in the process. Businesses should not be required to provide data on the use of low-risk ADM such as spreadsheets, transcriptions, spell check, and navigation systems. Examples of high-risk applications of ADM technology would include instances where ADM is making a final decision on matter of significant importance, such as medical benefits, housing, employment, or education. Regulating only final decisions is essential if businesses are to continue to serve consumers at scale using sophisticated algorithms which ultimately reduces cost and increases customer satisfaction.

- **Exempt applicant, employee, and independent contractor information.** The Agency should recognize permanent exceptions in ADM regulations for personal information of job applicants, employees, and independent contractors collected and used solely in the context those roles. This is consistent with the purpose and intent language of CPRA, which states that its implementation should "tak[e] into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses."[5]

- **Exempt information trade secrets and confidential information.** The agency's regulation ADM should not require businesses to divulge trade secrets or other confidential information. Such information is not personally meaningful to the consumer but can have adverse consequences for businesses. Moreover, any ADM or profiling information submitted to the Agency should be exempt from public inspection and copying under the California Public Records Act and be deemed not to constitute a waiver of any attorney-client privilege or work product protection.

- **Exempt ADM processes that directly relate to fraud prevention and security.** Regulations should exempt activities that specifically relate to the prevention of fraud and financial crime, defending legal claims, or any other type of security or compliance activities conducted as a routine practice by business.

[5] Proposition 24, CPRA, Section 3(A)(8).

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

- **Regulations should not be overbroad as to what constitutes ADM or profiling.** ADM technology is widely used, low-risk, and provides many benefits, such as word processing, email spam filtering and autocorrect. The Agency should avoid overly broad rules that impede the availability of such tools. Similarly, the Agency should not regulate "profiling" so broadly that low-risk activities such as movie recommendation and video streaming services are interrupted.

- **Regulations should be limited to personal information and use specificity.** ADM and profiling regulations should be limited to processing of personal information only. The Agency should also narrow regulations by focusing on specific, known harms rather than generalizations or by applying them only to high-risk, fully automated final decisions with a substantive impact on the consumer. Alternatively, the Agency can offset broader regulations with narrow and specific information, access, and opt-out requirements.

- **Regulations should consider industry-specific issues and defer to existing industry regulations.** In promulgating rules around ADM and profiling, the Agency should examine individual business sectors and tailor rules to the unique aspects of each industry. The Agency should also ensure new regulations are consistent with existing industry-specific regulations and should not create duplicative requirements already required by another regulatory body. At the same time, the Agency should not single out particular industries for regulation – regulations should apply to all industries.

- **Purely administrative functions should not be included under ADM.** Administrative decisions made with the use of ADM and profiling should be excluded from the regulations, such as machines that perform the same function as a human, only at a faster pace. For example, a machine that routes mail or phone calls, standard practice for several industries, should not be subject to regulation under CPRA.

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.

- **Website portals and disclosures should suffice for consumer access.** Businesses should be able to meet consumer access obligations for ADM and profiling process Information through website disclosures and regularly used self-help and other online methods currently used to allow exercise of rights under CCPA.

- **Technology deployers should be responsible for consumer access requests.** Regulations should make clear that the responsibility for consumer information access is with the technology deployer (companies using technology to interact with consumers). Developers' only obligation regarding consumer access requests is to provide "reasonable" assistance to deployers, who have the sole responsibility of communicating with consumers.

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.

- **Logic information should be limited to general criteria.** When providing "meaningful" information about the logic involved in a decision, businesses should be permitted to offer a description of the general criteria or categories of inputs used and weight given in reaching a final decision of significant impact to the consumer, rather than information about specific or individual decisions. Businesses should be able to provide this information via a publicly available disclosure on their webpage. Detailed descriptions of any complex algorithms involved in automated decisionmaking will not provide the average consumer with "meaningful" information on the logic involved in the processing.

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

- **Consumers should not be able to opt out of low-risk ADM.** Automated technology has led to safer products, process scalability, increased efficiency, and huge cost savings; allowing individuals to opt out could severely hinder the ability to realize these advantages for both businesses and consumers. Additionally, allowing consumers to dictate how businesses use or don't use everyday technology would pose a tremendous hardship to companies.

- **For essential high-risk offerings, businesses should be given the option of demonstrating operational guardrails in lieu of an opt-out requirement.** Opt-outs should also not be required for high-risk, final decisions because consumers can typically opt out by simply declining to do business with the company.

  To the extent businesses have essential or critical high-risk business offerings where it is not reasonable or feasible for consumers to consider other options, businesses should have the choice to demonstrate the existence of operational guardrails that effectively rather protect consumer interests, rather than having to provide for an opt-out. Examples of guardrails include ongoing monitoring, rigorous testing, corroboration of results, and established appeals and complaint processes.

  If businesses choose to use opt-outs, regulations should clarify that consumer-opt out requests be directed to the *deployer* of the ADM technology, and the role of developer be limited to assisting the business with opt-out requests as needed.

- **Any substantive expansion of opt-out rights should be legislative.** The Agency should not create any substantive expansions of opt-out rights via rulemaking including to resolve ambiguities. Any new or expanded rights should be addressed through legislation.

3. Audits Performed by the Agency

In general, the Agency should incorporate the following overarching principles into audits performed by the Agency across all the identified topic areas. We spell out topic-specific guidance under the corresponding headings below.

- **Uniformity with global, federal, and other states' standards.** To avoid unnecessary complexity and burden for businesses, the Agency should ensure its audit requirements and processes are uniform with other states and conform with global and federal laws and regulations. Additionally, the agency, to the extent possible should allow audits performed by other regulatory bodies to satisfy Agency audits under CPRA.

- **Uniformity with existing state law and regulations.** In conducting audits, the Agency should also ensure consistency with California's existing laws and regulations impacting audits across a variety of industries.

- **Exempt applicant, employee, and independent contractor information.** The Agency should recognize permanent exceptions from audits for personal information of job applicants, employees, and independent contractors collected and used solely in the context those roles. Regular audits of such information would create undue burden for businesses. This is consistent with the purpose and intent language of CPRA, which states that its implementation should "tak[e] into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses."[6]

- **Exempt trade secrets and confidential information.** Agency audits should not require businesses to divulge trade secrets or other confidential information; redaction should be allowed. The transparency goal of CPRA would be frustrated if businesses lack assurance that compliance with documentation and disclosure requirements will not be used against them in future litigation. Moreover, audit information submitted to the Agency should be exempt from public inspection and copying under the California Public Records Act and be deemed not to constitute a waiver of any attorney-client privilege or work product protection.

a. What the scope of the Agency's audit authority should be.

- **Audit authority should be limited to identifiable risks supported by evidence.** The Agency's audit authority should be constrained to its specific, defined investigation powers. Audits should not become fishing expeditions – they should be limited to an identifiable risk and restricted to instances where there is evidence a business has misused consumer information or otherwise materially violated provisions of the CPRA and created harm or substantial risk of harm to consumers. The scope of the audit should be limited to addressing the alleged misuse or violation.

---

[6] *Id.*

b. The processes the Agency should follow when exercising its audit authority, and the criteria it should use to select businesses to audit.

- **Audits should occur no more than annually.** Audits should not be conducted until final regulations are adopted by the Agency and be tied to a defined investigation as noted under (a), but in no event should they be more frequent than annually.

- **Initiation of audit should be subject to Agency majority vote.** To initiate an audit, a majority vote of the Agency Board members should be required to approve the audit based on evidence alleging misuse of consumer data or violation of CPRA.

- **Businesses should receive reasonable notice prior to audit.** Rules should provide businesses with a reasonable timeframe to produce requested information, at least 30 days' notice prior to an audit to allow preparation time.

- **Businesses should have option of selection a third-party auditor.** Businesses should be given the option to bring in an independent third-party assessor, subject to approval by the Agency Board, to conduct the audit.

c. The safeguards the Agency should adopt to protect consumers' personal information from disclosure to an auditor.

- **Secure information exchange should be developed for transmission of data.** The Agency should provide a secure method to receive and exchange information with businesses that will not compromise data.

- **Agency should avoid accessing, compiling, or storing consumer data.** The Agency should formulate its audits to avoid access to, or compilation of, consumers' information without compelling reason. Where the Agency does collect consumer personal information, appropriate technical and organizational measures to protect the data should be documented, and the consumer data should be promptly deleted when no longer needed for Agency purpose.

4. 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.

- **Consumers' right to correct should be limited to basic information that is provably inaccurate.** The right to correct can be imperative for consumers when necessary to change inaccurate information preventing them from accessing credit, housing, employment, or educational opportunities. Outside of clearly defined areas that have high importance to most consumers, allowing unbridled access to correct could impose significant burdens on business. Consumers should not have right to demand revisions to opinions, observations, inferences, or conclusions.

- **Rules should require businesses make "commercially reasonable efforts" to correct data only when information is significant to the consumer.** There should be a balance between the amount of effort on the part of business to correct information versus the significant impact said data has on a consumer. An evaluation of what efforts are "commercially reasonable" for a business to take should be strongly influenced by the effect that the data may have on a consumer. For example, corrections to data that may determine a consumers' ability to obtain credit are significant, while altering a consumer's inaccurate purchase history does not have the same meaningful impact.

- **Flexibility for how a business handles data of minimal importance.** Businesses should have the option to delete inaccurate data instead of replacing it with other data when the significance of the data to the consumer is minimal (e.g., a correction on a credit report is more important than correcting purchase history).

- **Businesses should not bear the burden to independently ascertain whether data collected or produced in good faith is inaccurate.** Customers should be expected to provide evidence that information held by a company is inaccurate and businesses should be given leeway to establish reasonable procedures commensurate with the impact inaccurate data may have on a customer. Businesses should not be subject to constant relitigation of their good faith decisions that the evidence provided by a consumer is not sufficient to demonstrate that information is inaccurate.

- **Regulations should follow existing state law on data deletion.** California law already contains a deletion obligation that should not be overridden by the right to correct.[7]

b. How often, and under what circumstances, a consumer may request a correction to their personal information.

- **Significant information with high impact on consumers should be the focus.** Both businesses and consumers have a mutual interest in personal information being accurate. Regulations around how often a consumer can request a correction should be based on the type of information being corrected and the impact that information has on the consumer.

- **Existing methods for customer contact should suffice for correction requests.** To the extent that the business has in place existing methods to readily allow consumers to correct their personal information (e.g., contacting a call center, updating profile online) those current methods should be acceptable under CPRA. Creating new formal processes to make simple data corrections such as name, address, email, or phone number will produce poor customer experiences.

- **Rules should mirror CCPA regulations on "verifiable" requests.** The Agency should seek to remain consistent with CCPA regulations as they pertain to the concept of "verifiable" requests and adopt similar guidelines.

[7] Cal. Civ Code § 1798.105

c. **How a business must respond to a request for correction, including the steps a business may take to prevent fraud.**

d. **When a business should be exempted from the obligation to take action on a request because responding to the request would be "impossible or involve a disproportionate effort" or because the information that is the object of the request is accurate.**

- **Obligation to respond should be limited to corrections with significant impact.** In circumstances where the information is accurate, the business should not be required to take any action. Only in circumstances where a business owns, possesses, or controls misinformation should a business be required to act on such a request. In determining whether the request is impossible or would involve a disproportionate effort, the nature of the information in question should be considered. The more significant the information, the higher the obligation on the business.

- **Exemption for existing correction/deletion obligation.** Businesses that are required by other laws to maintain accurate information about consumers (and correct such information) should be exempt from the correction requirement(s).

e. **A consumer's right to provide a written addendum to their record with the business, if the business rejects a request to correct their personal information.**

- **Exemption for existing regulations on consumer information accuracy.** To the extent a business is subject to other regulation requiring investigation of accurate personal information, they should be exempt from additional regulations.

- **Exemption for existing contractual relationship.** Where a preexisting contractual relationship exists between a business and a consumer, the consumer should not be able to use the correction request under CPRA to alter existing obligations.

- **Exemption for applicant, employee, and independent contractor information.** Allowing applicants, employees, and independent contractors to delete information from their workplace record would have significant negative consequences when it comes to complying with state and federal employment laws. It could also put businesses in a vulnerable position should they need to defend against future legal claims from the employee.

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**

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

- **Information necessary to establish and maintain a business functions between a business and consumer should be excluded from limitation.** Regulations limiting the use of sensitive personal information should not apply to data that has been

deidentified or if use and disclosure is (1) necessary to complete a transaction between a business and consumer, (2) essential for the business to service or maintain a consumer's account, and (3) reasonably contemplated by the consumer for business use.

- **Exclusions should apply for activities related to fraud-prevention and security.** There should be exemptions for any processing relating to fraud prevention, anti-money laundering processes, screening, or for other type of security or compliance activities.

- **Opt-ins should be allowed for customers who previously opted out.** Regulations should outline a method by which customers who previously opted out can opt back in for specific use cases for specific businesses.

- **Exemption for sensitive personal information for applicants, employees, and independent contractors.** There should also be exemptions for personal information in the context of workplace relationships. Regulations should: (1) not impose undue burden; (2) permit an opt-out process through existing internal human relation 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.

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.

- **Agency should uphold businesses' choice between opt-out web links or a global opt-out signal.** CPRA provides businesses can but are not required to allow consumers to use a global opt-out signal. Specifically, businesses can still (a) provide clear and conspicuous opt-out links on their website or (b) allow consumers to opt out through a "preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]"[8]

  The CPRA goes out of its way to emphasize the ability of businesses to choose between the two methods, stating. "A business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b)."[9]

  The Agency's regulations should recognize and remain consistent with this business choice under CPRA as well as incorporate the items set forth in CPRA section 1798.185(a)(19)(A).

[8] Cal. Civ. Code § 1798.135(a), (b)(1), (3).
[9] *Id.* at (b)(3) (emphasis added).

- **The global opt-out function needs to be standardized before its validity is recognized by the Agency.** Currently, browser-based opt out technology is not sufficiently interoperable or developed to serve as a reliable indicator of consumer choice. The uncertainty around using a single globally recognized option exists because there are no guiding principles regarding its creation, implementation, universality, or the ability to ignore it when appropriate. Businesses need a standardized system with clearly defined exemptions when such an option would pose a broad risk to consumer data security.

- **Global privacy control standards should be developed with broad business sector feedback.** The universal signal should be developed with input from the industries across all business sectors so that no one entity exerts more influence than another over the signal's standards. Any resulting regulations should provide businesses with the flexibility to implement various technical solutions that fit their business needs rather than mandating a single type of solution.

- **Global opt-out standards should provide consumers with notice and indicate whether they are in California.** Any global opt-out technology should ensure consumers are making an informed choice by notifying them that about what a "Do Not Sell" means in California rather than use defaults of which the consumer may not be aware. Businesses must also have the means to accurately determine whether the consumer is located in California. Businesses should not be required to identify unauthenticated users.

- **Businesses should only have responsibility to opt out recognized customers.** The rules should specifically state that businesses are only responsible to record notifications from recognized customer's internet protocol (IP) addresses as it would be nearly impossible for businesses to accurately identify individual users on every IP address or device and distinguish between them for purposes of a universal opt out. Even with an ability to opt out, new rules should not restrict a business's ability to use its data for legitimate business purposes agreed to by contract where personal information will not be sold but only used by the service provider to deliver services.

- **Businesses should be allowed to request customer permission to use website "cookies".** To provide consumers with the ability to make educated decisions regarding their privacy, businesses must be allowed under the rules to notify consumers of the consequences of an opt-out and be able to request permission to use a customer's "cookies" (e.g., data about which websites a consumer visit online).

- **Regulations must be explicit with respect to what "sharing" includes in the context of opt outs.** The CPRA specifies 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 but does not specify what sharing of personal information means. For instance, the Agency should clarify that in scenarios where customer information is passed to another party for purposes of targeted advertising, and the data is not enhanced in any way or used for any

other purpose, this does not constitute sharing under CPRA's service provider business purpose exception.

c. How businesses should process consumer rights that are expressed through opt-out preference signals.

- **Regulations should only require businesses be responsible for opt outs from IP addresses or devices from which the signal has been sent.** Businesses should not be required to distinguish between users at the same IP address or on the same device; it would be impossible to accurately associate the opt out request between different persons under those circumstances. Given the private right of action under the CPRA, requiring businesses perform an impossible task only sets them up for frivolous and unavoidable lawsuits. This would be especially true for small and medium sized businesses.

- **Rules should provide flexibility for business to use existing opt out functions.** the rules should also avoid being too prescriptive in what must be used as an opt out solution, such rigidity would surely limit future business innovation and eventually customer opt out options.

- **The opt out option should be limited to online data collection.** it would be a burden to require a business to identify unauthenticated users for purposes of ensuring they are opted out of all forms of personal information sales.

f. 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.

- **Sufficient flexibility should be provided to enable business to use existing processes.** Regulations should outline a method by which customers who previously opted out can opt back in with specific businesses for specific purposes and allow businesses to use existing online functions for such purposes.

6. Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information

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.

- **Information to establish identity should not be subject to the right to limit use and disclosure.** This should include the use of personal information (including biometric data) solely for establishing identity.

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.

- **Use or disclosure should be allowed in cases of opt-in consent or when reasonably necessary for requested service.** Any rules regarding the use of sensitive personal data should not apply in circumstances where a consumer has given opt-in consent to use the data, or such use is reasonably necessary to provide the service the consumer has requested. To the extent data is necessary for the day-to-day operation of a business, or is currently permitted or required by law, such use should also be permitted notwithstanding the consumer's direction to limit use.

- **Exemption for fraud prevention, security, and employment/independent contractor relationships**. Sensitive personal data used in routine business functions such as improving quality of service or company security or consumer information protection processes, including fraud prevention, anti-money laundering processes, and compliance activities should not be classified as sensitive data. Also, such information collected from applicants, employees, or independent contractors should be excluded from limitations on use or disclosure to prevent potential conflict with state and federal employment laws and preserve the ability to exercise or defend against legal claims.

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

a. **What standard should govern a business's determination that providing information beyond the 12-month window is "impossible" or "would involve a disproportionate effort".**

- **Information archived or beyond a 12-month window should be deemed impossible to provide.** Allowing consumers to ask for data collected beyond a short and defined window serves no purpose other than to provide more burden on business for likely outdated information.

- **Exclusion for information provided by the consumer.** There should be a limitation on requests to provide information given directly to the business by the consumer. A business should not have to spend resources providing information to a consumer which the consumer gave voluntarily.

8. **Definitions and Categories**

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

- Household should be removed, the definition should be for individuals, not households, devices, IP addresses, etc.

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

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

d. Changes, if any, that should be made to the definition of "designated methods for submitting requests" to obtain information from a business.

- **Methods should be discretionary.** The methods consumers use to submit requests to businesses should be at the discretion of the business and not prescribed by the state. Businesses should be required to make the submission process accessible (e.g., consumers should be able to submit requests online) and not cumbersome (e.g., should be convenient to request on a business's website).

- **Use of service providers.** Businesses should be able to designate or contract with a third-party service provider to maintain methods for receiving and processing submission requests.

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

- **Exemption for fraud prevention, security, and employment/independent contractor relationships**. Sensitive personal data used in routine business functions such as improving quality of service or company security or consumer information protection processes, including fraud prevention, anti-money laundering processes, and compliance activities should not be classified as sensitive data. Also, such information collected from applicants, employees, or independent contractors should be excluded from limitations on use or disclosure to prevent potential conflict with state and federal employment laws and preserve the ability to exercise or defend against legal claims.

f. The changes, if any, that should be made to further define when a consumer "intentionally interacts" with a person.

g. The changes, if any, that should be made to further define "precise geolocation."

- **Exclude business operations that benefit consumers.** The CPRA expressly allows businesses to use precise geolocation for operational functions that benefits all consumers, and this should be reflected in the definition.

- **Exclude geo fences.** Also, the definition or precise geolocation should exclude entry/exit into a "geo fence." A geo fence is a virtual geographic boundary, defined by GPS or RFID technology, that enables software to trigger a response when a mobile device enters or leaves a particular area. Geo fences are typically something customers specifically opt into to trigger a convenient function, but the purpose is not to physically track a customer's location.

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

i. The regulations, if any, that should be adopted to further define "law enforcement agency-approved investigation."

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

- **Focus definition on practices that constitute consumer fraud.** The CPRA definition of "dark patterns" is potentially overinclusive as any user interface that creates structure by establishment of a user-flow experience could be interpreted as having the effect of limiting user "choice" to the options that are provided. Designers must necessarily make choices in creating user experiences and attempting to design an interface that provides a user with control over every theoretical choice that could exist in the context of a service would be impractical. The regulations should support clarity by specifying the definition of "dark patterns" is focused on design practices that amount to consumer fraud.

9. Additional Comments

- **Regulations should clarify what constitutes "cure."** What constitutes "cure" was not defined in the CCPA, and CPRA added a sentence that the "implementation and maintenance of reasonable security procedures and practices . . . following a breach does not constitute a cure with respect to that breach."[10] If this does not constitute a cure, it is not clear what does. Absent clarifications, "cure" under CPRA is not meaningful. We urge the Agency to address this as the opportunity to cure is critical to businesses in mitigating unnecessary and costly litigation.

- **Reasonable implementation periods for regulations and modifications to regulations.** Given the complexity and burden of implementing new regulations, the Agency should state the regulations and modifications to regulations that businesses have at least six to 12 months from final adoption of the regulations to implement them before they are enforced.

In conclusion, CJAC urges the Agency to create regulations that are clear, balanced and in harmony with existing laws and regulations. This will facilitate implementation of and compliance with the CCPA and CPRA and avoid unnecessary enforcement actions and private litigation, while protecting consumers and carrying out the intent of these privacy statutes. Again, we appreciate the opportunity to provide preliminary comments and are readily available to answer any questions you may have.

Respectfully Submitted,

Kyla Christoffersen Powell
President and Chief Executive Officer

[10] Cal. Civ. Code § 1798.150(b).