From: Cynthia Pantazis[redacted]
Sent: 11/8/2021 3:34:30 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: Goole comments - CPRA - November 8, 2021 (1).pdf

[EXTERNAL]: [redacted]

Enclosed please find Google's comments on proposed topics of CPRA rulemaking.

Thank you.

--
Cynthia Pantazis
Director, State Policy
Google LLC

By email

November 8, 2021

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

To Whom It May Concern:

Please find below Google's comments with respect to the September 22, 2021 Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act ("CPRA") of 2020. We thank the California Privacy Protection Agency ("Agency") and staff for considering these comments and for providing businesses with needed clarity on the law.

1. Overarching Priorities for Achieving the CPRA's Regulatory Objectives

As the Agency considers input from stakeholders in achieving the law's regulatory objectives in the most effective manner, we support its efforts to provide businesses with clarity on complying with the CPRA. To that end, we offer the following overarching priorities for the Agency to consider as it moves forward in the rulemaking process:

(1) Prioritize providing clarity to businesses around the new obligations established by the CPRA rather than introducing additional obligations shortly before the law takes effect. Over time and with more information, the Agency will be positioned to assess whether further changes will be beneficial for consumers;

(2) Seek to align the CPRA's requirements with other, compatible privacy requirements to best facilitate consumer understanding and to promote privacy-preserving business practices; and

(3) Provide flexibility for businesses to respond to consumer requests in a manner that prioritizes substance over form.

Prioritizing Clarity: Notwithstanding any further regulations that the Agency may adopt, the CPRA imposes a number of new obligations on businesses that require significant work to prepare for. The timeline for adopting final regulations on the twenty-two areas identified in the CPRA is July 1, 2022, and those regulations will be effective only six months later on January 1, 2023 and enforceable on July 1, 2023.[1] We urge the Agency to allow businesses adequate time to bring their practices into compliance with the CPRA's baseline requirements by 2023 before considering additional substantive changes. If time and experience indicate that the law as drafted leaves consumers insufficiently protected, the Agency can address those needs in the future. For example, while the law permits regulations to update certain core definitions (including what constitutes "personal information", "sensitive information", "service provider", and "business purposes"), we urge the Agency not to adjust these core definitions without the benefit of more time to review compliance and enforcement.

Alignment with Other Laws: Regulations should, to the extent possible, align the CPRA's requirements with other privacy laws' requirements that advance the same policy goals. Indeed, the law's Findings and Declarations acknowledge that "[t]o the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions."[2] Further, an Agency function under the CPRA is to "[c]ooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections."[3] To that end, the Agency should, to the fullest extent possible, align its regulations with the requirements imposed under other laws.

Since the CPRA was passed, Colorado and Virginia have each passed their own comprehensive consumer privacy laws, both of which will also take effect in 2023 and will impose substantively similar business obligations, including to: (1) provide notice of privacy practices; (2) allow consumers to access, delete, and correct their information; and (3) opt out of the transfer of their information for targeted advertising purposes. These new state laws add to existing privacy regulations in other jurisdictions, such as the GDPR in the European Union, with which many businesses operating in California also must comply. The best way to advance businesses' compliance with the CPRA is to ensure that compliance obligations are, to the extent possible, consistent with the parallel obligations of these and other privacy laws. In other words, businesses should be able to meet similar compliance obligations across the US and globally via the same mechanisms and processes. The alternative of highly specific and detailed regulations to meet obligations imposed only in California would force businesses to maintain different privacy disclosures, practices, and user controls for different states and countries, even when the basic information, protections, and rights are consistent. Not only would such efforts be costly, error-prone, and burdensome, they would actually undercut consumer understanding and lead to more confusion.

---

[1] California Civil Code § 1798.185(d); CPRA § 31.
[2] CPRA § 3.C.8.
[3] California Civil Code § 1798.199.40(i).

Highly specific or conflicting obligations would also run counter to the law's data minimization requirements by potentially requiring businesses to collect *more* information to understand the residency of their users, or to seek to adopt imperfect technical measures to attempt to determine the location of the visitors to their websites and other online services.

As specific examples of alignment with other laws, businesses should be given flexibility in how they respond to consumer requests provided those responses meet the substantive requirements of the CPRA. Similarly, to the extent possible, the Agency should align rules regarding permissible uses and combining of personal information by service providers and contractors with other laws that regulate the relationship between similar classes of entities, to enable consistency of contracts and data protection terms between businesses and their vendors.

Supporting Flexibility: In issuing regulations concerning businesses' responses to consumer rights requests, the Agency should promote flexibility to meet the policy objectives of the law and not impose overly prescriptive obligations that would prioritize form over substance. For example, the Agency should embrace the law's mandate that "[c]onsumers or their authorized agents should be able to exercise these options through easily accessible self-serve tools."[4] To that end, rather than forcing businesses into uniform wording or procedures, the Agency should recognize self-serve tools that many companies have built to provide consumers access to and the ability to delete their information and to exercise choice with respect to the use and disclosure of their information independent of any mandate imposed by California law.

The regulations should similarly provide businesses flexibility in responding to requests to know the specific pieces of information held about them. As mandated by the law, the Agency should define this standard "with the goal of maximizing a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, such as system log information and other technical data."[5] The Agency should, in this regard, ensure that its regulations align with the law's requirement that businesses not be required to link information that is not kept as personal information in the ordinary course of business; retain information that they would not ordinarily retain; maintain information in an identifiable or linkable form; or collect, retain, or access any data or technology, for the purpose of being able respond to consumer requests.[6]

Similarly, in issuing regulations concerning opt out signals sent by platforms or other technologies, the Agency should aim to provide businesses clarity so that they understand what signals they must look for and how to respond to them. Google recognizes that these signals will be an important means for users to indicate their preferences. And to make this system work effectively, the Agency must be clear about which automated signals must be honored under the law and how new signals will be approved. For instance, the Agency could adopt an approval process under which it evaluates new opt out tools against clear criteria. At minimum, the

---

[4] CPRA § 2.
[5] California Civil Code § 1798.185(a)(14).
[6] California Civil Code § 1798.145(j).

Agency should make clear the criteria required for a signal to be considered a valid opt out signal. Similarly, the Agency should make clear its expectations for businesses when they receive an opt out signal but have an existing relationship with and/or consent from a consumer that might conflict with the signal. Finally, in the context of particular uses of sensitive information, the Agency should clarify how automated signals should be used, how it intends for businesses to respond to such signals, and that any such signals may be distinguished from those used to opt out of sales and sharing of personal information.

Finally, with respect to what information businesses must provide in response to a right to know request, the Agency should recognize (as the AG did with respect to the CCPA regulations) the risks related to providing such information in response to a request to know, particularly where the requesting individual is not signed into an authenticated account with the business, and, also, the higher standard of authentication that the CPRA acknowledges may be required for more sensitive personal information.[7] Requiring businesses to provide highly sensitive information without robust verification processes would expose consumers to potential harms rather than serve the law's goals of protecting them.

In addition to the overarching priorities that we have outlined above, we also provide the following responses on the specific topics about which the Agency has requested comments.

2. Recommendations for Audits Performed by Businesses and by the Agency

The Agency has requested comments concerning the circumstances under which businesses must perform cybersecurity audits and report risk assessments to the Agency.[8] On this topic, we provide the following observations for the Agency to consider.

Significant Risk to Consumers' Privacy or Security: On the issue of what type of processing of personal information presents a "significant risk to consumers' privacy or security," we urge the Agency to look to, and align with, privacy and data security laws that also address risk of harm in certain processing. For example, state data breach reporting laws require businesses to report security breaches with respect to certain categories of information precisely because such information, in the wrong hands, may pose a significant risk to consumers' privacy and security. Looking at the type of personal information covered by those laws, including California's own breach reporting law, will allow the Agency to identify the types of processing most likely to pose a significant risk to consumers' privacy and security. Aligning audit requirements to cover the same processing that is subject to data breach reporting obligations would, in essence, ensure that personal information that is presently subject to special protections *after* a breach occurs is subject to proactive review in order to make a breach less likely. Such a standard would also align with existing privacy and security laws that require reasonable security based on the sensitivity of the data, and would incentivize companies to redact and encrypt data where appropriate.

---

[7] California Civil Code § 1798.185(a)(14).

[8] *See* Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020, *available at* https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

Processes for Cybersecurity Audits & Risk Assessments: On the subject of performing cybersecurity audits and submitting risk assessments, Google urges the Agency to ensure that any such audits and assessments required under the law are protected by strict confidentiality provisions that prevent disclosure to or use by unauthorized third parties. Threats to the confidentiality of audit or assessment results would undermine, rather than serve, the goals of the law by disincentivizing businesses from engaging in a thorough review and also by potentially exposing consumers to security breaches if such results were to be accessed by malicious actors. In issuing its regulations, the Agency should, moreover, consider the multitude of audits, assessments, and similar reviews to which businesses are already subject and ensure that any audit and assessment obligations imposed under the CPRA allow businesses to use or repurpose reviews conducted under other legal regimes or widely-accepted industry standards or frameworks that advance the same privacy and security goals as the CPRA.

3. Automated Decisionmaking

The Agency has asked for comment regarding its authority to issue regulations concerning automated decisionmaking, including: what activities should be deemed to constitute "automated decisionmaking technology"; consumers' access rights concerning businesses' use of automated decisionmaking technology and what businesses must do in order to provide "meaningful information about the logic" involved in the automated decisionmaking process; and the scope of, and process for facilitating, opt out rights with regard to automated decisionmaking.

Google urges the Agency to align any definition of automated decisionmaking with existing law and, specifically, to focus any rules concerning automated decisionmaking on fully automated decisionmaking that produces legal effects or effects of a similar import, such as a consumer's eligibility for credit, employment, insurance, rental housing, or license or other government benefit.

A standard focused on decisions of legal or similarly significant effect would be consistent with other global and domestic privacy standards and would serve consumers' interests by highlighting those decisions most likely to have a meaningful impact on them. Articles 15 and 22 of the GDPR, for example, provide data subjects transparency rights with respect to automated decisionmaking only to the extent such decisionmaking produces legal or similarly significant effects. Similarly, Colorado and Virginia's new omnibus privacy laws (which will also take effect in 2023), govern "profiling" only to the extent such profiling is in "furtherance of decisions that produce legal or similarly significant effects concerning a consumer."[9]

These laws' focus on decisionmaking that has the potential to produce substantial harm is well-considered. As recognized by the drafters of the GDPR, there should be, subject to some exceptions, additional protections around decisions that materially impact consumers' lives, "such as automatic refusal of an online credit application or e-recruiting practices" or involved in the analysis or prediction of "aspects concerning [a] data subject's performance at work,

[9] *See* Colo. Rev. Stat. § 6-1-306(1)(a)(C); VA. Code Ann. § 59.1-573(A).

economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her."[10] There is no compelling policy justification for extending the same restrictions to machine learning practices used to, for instance, choose the language in which information is presented or to determine the driving directions provided to a consumer.

We appreciate the opportunity to provide preliminary comments on proposed topics of CPRA rulemaking.

Sincerely,

Cynthia Pantazis
Director, State Policy

[10] GDPR Recital 71.

From: Leticia Garcia [redacted]]
Sent: 11/8/2021 3:49:36 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 California Grocers Association
Attachments: CPRA CGA 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 afternoon,

Please find attached the public comments from the California Grocers Association. Thank you!

Leticia Garcia
Director, State Government Relations
California Grocers Association

Cell [redacted]
Address 1005 12th Street Suite 200, Sacramento, CA 95814
Website www.cagrocers.com

cga

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

Dear Ms. Castanon,

On behalf of the members of the California Grocers Association (CGA), I write to express concerns with the proposed updated language to the CPRA.

CGA is a non-profit, statewide trade association representing the food industry since 1898. CGA represents approximately 500 retail members operating over 6,000 food stores in California and Nevada, and approximately 300 grocery supplier companies. Traditional supermarkets in California employ more than 300,000 residents in virtually every community in the State.

Automated Decisionmaking

Automated decisionmaking 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 of a broad category 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. Every day technology like calculators, word processing software, and scantron machines could be considered automated decisionmaking technology. Even newer and more complex automated decisionmaking technology, like artificial intelligence, is used routinely in business and includes things like email spam filters and autocorrect features.

Automated decisionmaking technology and profiling should be limited to activities that require the processing of personal information. Personal information should be defined in alignment with the CPRA and subject to the exceptions described in the law. Such focus on personal information is consistent with the overall focus of the CPRA on consumer privacy.

Automated technology has significant benefits to both businesses and consumers, including enhanced accuracy and consistency, safer and more innovative products, scalability, cost savings, and increased efficiency. Accordingly, regulators should be very mindful about providing consumers any right to opt out of automated activities, as it could severely hamper businesses' and other consumers' ability to realize those advantages.

Businesses should not be required to provide information on use of low risk automated decisionmaking technology, such as spell check, GPS systems, databases, spreadsheets, or transcription services. Requiring businesses to provide information on such low risk technology could slow down their activities substantially, while not providing a meaningful benefit to consumers, who should expect that business activities are performed using well-accepted, widely used technology.

Specifically in the grocery business, our members are not in a business where tracking such information is their field of expertise. The decisonmaking technology that is used provides better access of groceries to their customers. Adding this additional tracking of information will take away resources to other necessary services that grocers provide, such as philanthropic endeavors, additional store locations, etc.

A more detailed description of any complex algorithms involved in automated decisionmaking will not provide the average consumer with a "meaningful" information on the logic involved in the processing. In addition, providing a detailed explanation of the algorithms involved runs the risk of imposing obligations that conflict with the intellectual property, trade secret, and other legal rights of the business in question.

Given the nearly infinite range of uses of automated decisionmaking technology in everyday tasks, a generic, one-size-fits-all approach to information is impractical and could prevent/slow business and consumer access to useful tools. Instead, California should tailor any regulation regarding when consumers should be able to access information about businesses' use of automated decisionmaking technology to high risk, final decisions that are fully automated (e.g., no human in the loop).

Further, regulating only final decisions is critical to enable businesses to serve consumers at scale. For example, individuals receive faster access to services if businesses can quickly identify low fraud risks. This is only possible at scale using either simple algorithms – e.g., approve transaction with no prior fraud flags – or more complex algorithms including ones using machine learning. Then, for the smaller set of fraud risk cases, businesses can use manual review to make final decisions, for example through an appeals process. In these situations, if non-final decisions – e.g., cases flagged only by algorithms for further human review – are regulated, then consumers will receive slower access to services, and will incur higher costs from increased, and unnecessary, manual review.

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

The right to correct can be an important tool for consumers when necessary to correct inaccurate information that may be preventing them from accessing credit, housing, job or educational opportunities. But outside of those defined areas and untethered from a rule of reason, it could have a profound impact on free expression and impose a significant burden on businesses.

The processing of personal information in the HR context should be excluded from such regulations. Any risks to the privacy of individuals in the HR context is far outweighed by the burden such regulations would place upon businesses in the HR space. Regulations would result primarily in significant confusion and cost, conflicts with a litany of federal and state employment laws governing personal information in the HR space, and impair the ability to

exercise and defend against legal claims.

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

Sharing & Sale

There is uncertainty right now with the universal opt-out signal because there are no guiding principles regarding its creation, implementation, universality, and the ability to ignore it when appropriate. The universal signal should not be left to the devices of any single organization to create. It should be created with the required input from the industry so that no one entity exerts outsized influence over the signal's standards. Doing so would keep the number of signals to a minimum (ideally one) so there would be no conflicts among signals if each one had different standards and if customers sent conflicting signals. The signal needs to apply only to recognized customers and be applicable across browsers and devices. It should also allow customers to opt in/reverse any opt out selection. Without these requirements, the industry risks multiple entities creating differing signals using varied standards and places significant compliance costs upon businesses.

Grocers are not in a business where they profit off the data of their customers. Having a blanket approach to the opt-out process could pose difficulties and could lead to additional costs passed down to the consumer. This would not be beneficial to grocers if they have to raise prices during a time when grocery prices are steadily raising.

Meaningful privacy protections cannot exist without a clear understanding of what the privacy rules are meant to protect. The statute is clear that when "sharing" for cross-context behavioral advertising, businesses need to offer an opt-out or honor the universal signal, but it fails to clarify or offer examples of that term. The apparent purpose of including "sharing" in the CPRA is to capture the transmission of personal information for profile-building purposes. It should therefore not include circumstances where personal information is passed to another party for targeted advertising purposes but is not enhanced by or otherwise decorated with another party's personal information. If an ad server delivers an ad campaign, certain device or other information needs to be passed to the ad server. That information is not used for any other purposes, and it is not enhanced with other data before being used to deliver the ad, then that passing of data should not be "sharing." Regulations must be explicit in reflecting this meaning. If this scenario is what the service provider business purpose exceptions contemplate in the CPRA, then the regulations need to explicitly confirm.

Regulations should outline a method by which customers (who previously opted out) have the ability to opt in for specific use cases for specific businesses.

Use and Disclosure of Sensitive Personal Information

There should be appropriate carve-outs for any processing relating to fraud prevention, anti-money laundering processes, screening, or for other type of security or compliance activities. Companies often must work with third party service providers to support these activities, so providing a

customer the opportunity to opt out would substantially hinder companies' ability to protect customers.

Further, regulations should outline a method by which customers (who previously opted out) have the ability to opt in for specific use cases for specific businesses.

For HR – The processing of personal information in the HR context should be excluded from such regulations. Any risks to the privacy of individuals in the HR context is far outweighed by the burden such regulations would place upon businesses in the HR space. Regulations would result primarily in significant confusion and cost, conflicts with a litany of federal and state employment laws governing personal information in the HR space, and impair the ability to exercise and defend against legal claims. Further, "sensitive personal information" collected in the HR context is primarily not collected to "infer[] characteristics about a consumer," but rather for a variety of legitimate purposes in order to comply with state and federal laws. Accordingly, "sensitive personal information" should also be excluded from regulations in the HR space. Regulations in the HR context, if any, 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.

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

"Sensitive personal information" 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 should include the use of personal information (including biometric data) solely for establishing

Specific to the grocery industry, social benefits like SNAP have expanded into online shopping and WIC is soon to follow. Federal requirements on data collection and storage on these programs need to be taken into consideration given the use of it to evaluate these programs.

There should also be appropriate carve-outs for any processing relating to fraud prevention, anti-money laundering processes, screening, or for other type of security or compliance activities. Companies often must work with third party service providers to support these activities, so providing a customer the opportunity to opt out would substantially hinder companies' ability to protect customers.

For HR – "Sensitive personal information" collected in the HR context is primarily not collected to "infer[] characteristics about a consumer," but rather for a variety of legitimate purposes in order to comply with state and federal laws. Accordingly, "sensitive personal information" should be excluded from regulations in the HR space. Nonetheless, regulations in the HR context, if any, must "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," Cal. Civ. Code § 1798.100(A)(8), in order to avoid prevent undue burden, to prevent potential conflict with state and federal employment laws, and preserve the ability to exercise or defend against legal claims.

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

Privacy standards should be consistent across state lines. There are several members, small to larger store brands, that operate in other states. Specifically our independent operators on the state border, they do not necessarily have the bandwidth to implement multistate compliance when there are costumers that may cross state boarders to purchase groceries in California.

As such, we suggest aligning any data impact or risk assessments aligned with other laws that will come into effect in 2023, such as the Virginia Consumer Data Protection Act's (VCDPA) and the Colorado Privacy Act's Data Impact Assessment. The proposed assessment focuses on key issues such as the sale of personal data and the use of personal data in the context of targeted advertising, however it also provides controllers with the flexibility and ability to determine what is considered a significant risk to consumers based on their product or service. A consistent standard for data impact assessments and cybersecurity audits should be synonymous across state lines to allow for businesses to continue to build robust systems to protect consumers information. These systems will benefit from clear guidelines that allow businesses to innovate and develop their data protection assessments and properly assess their cybersecurity risks.

From a security risk perspective - this provision should be limited to processing of data that, if compromised, is likely to result in real, concrete harms to individuals. Examples may include identify theft/fraud, extortion, or physical injury from disclosure of intimate or other objectively sensitive personal details (e.g., sexual orientation).

From a privacy risk perspective – this provision should be limited to processing that has a legal or similarly significant effect on an individual- i.e. where the impact will produce a decision that will impact housing, education, employment and other areas protected from discrimination under the law.

In the HR context, the processing of most "personal information" (which is defined in the CPRA to include "sensitive personal information"), does not present a "significant risk to [individuals'] privacy or security"—particularly where the CPRA states that it shall not apply to personal information that is collected by a business in the context of job applicants and employment/independent contractor relationships to the extent that the personal information is collected and used solely within the context of individuals' role or former role as a job applicant, employee, or independent contractor—including, but not limited to, emergency contact information and information necessary to administer benefits. *See* Cal. Civil § 1798.145(m)(1). Therefore, the processing of "personal information" in the HR context should not be the subject of required annual audits or regular risk assessments. Annual audits or regular risk assessments in the HR context, if any, should be voluntary. Finally, requirements in the HR context, if any, 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," Cal. Civ. Code § 1798.100(A)(8)—most notably, existing state and federal requirements which require businesses to collect and retain employment related records for a litany of compliance and reporting purposes. In sum, regulations relating to personal information in the HR space will only result in confusion, conflicts with existing state and federal requirements, and undue burden upon businesses.

Businesses should not be required to use third party auditors as the burden and expense would be wildly disproportionate to any downstream consumer benefit, and the result would likely be increased consumer costs. Self-audit is more appropriate; many businesses already have self-audit mechanisms using appropriate industry standards and they should be able to leverage those existing processes to meet CPRA requirements.

Some businesses may also already perform certain industry standard audits and reports. For example, storage of payment cards on file is regulated in the industry by the PCI-DSS standards

and merchants are required to re-certify every year. In those circumstances businesses should be able to re-use such audits/certifications rather than duplicate their efforts, which would unduly add to the cost and burden of compliance.

Further, businesses should be permitted to use certifications and audits related to cybersecurity from service providers to help meet their requirements to conduct cybersecurity audits and provide risk assessments.

For HR – For the reasons stated above, the processing of personal information in the HR context should be excluded from regulations requiring annual security audits. Annual security audits in the HR space, if any, should be voluntary. Finally, requirements in the HR space, if any, 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," Cal. Civ. Code § 1798.100(A)(8), to prevent undue burden, and reduce conflicts with state and federal employment laws.

The potential burden and expense of extensive risk assessment requirements should be balanced against any downstream consumer benefit, so that they don't lead to increased consumer costs. Specifically, risk assessment should be limited to the high-risk processing in question and NOT cover all processing activities of the company.

The regulations should recognize that risk assessments are an increasingly common requirement under U.S. and international privacy and data protection laws. In order to promote interoperability and minimize burdens to covered businesses, the regulations should specify that the Agency will accept risk assessments that were originally conducted pursuant to a comparable legal requirement.

The regulations should further recognize that a single risk assessment may address a comparable set of processing operations that include similar activities.

In providing guidance for conducting risk assessments and weighing the benefits of processing against potential risks, the regulations should provide that the factors relevant to this balancing may include:

- Technical and organizational measures and safeguards implemented by the business to mitigate privacy and security risks
- The reasonable expectations of consumers
- The context of the processing with respect to the relationship between the business and consumers

Risk assessments should highlight the most significant privacy risks associated with the processing activity in question and the steps being taken to address and mitigate that risk – should not require the company to divulge commercially sensitive information.

The regulations should not require organizations to repeatedly conduct or submit 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. Therefore, the Agency's regulations should specify that businesses are only required to "regularly submit" assessments for new or materially changed processing practices that

present a significant risk.

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 conducted 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.

For HR – For the reasons stated above, the processing of personal information in the HR context should be excluded from regulations requiring submission of risk assessments to the Agency. Risk assessments in the HR context, if any, should be voluntary. Finally, requirements in the HR space, if any, 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," Cal. Civ. Code § 1798.100(A)(8), to prevent undue burden, and reduce potential conflicts with state and federal employment laws.

Audits Performed by the Agency

We are not aware of other similar agencies or AGs with rights to audit businesses for privacy or security issues beyond their specific, defined investigation powers. So it is important that this audit power is appropriately constrained by the regulations. Specifically, audits should not be come fishing expeditions – their scope should be clearly defined by the Agency and responsive and limited in scope to an articulable risk or issue.

Audits should not be conducted until final regulations are adopted by the Agency and should occur no more than annually for any business subject to the requirements.

The Agency should formulate its audits to avoid access to or collection of consumers' information, unless absolutely necessary – it should not collect consumer information without a compelling need for it.

The Agency should provide a secure method to receive and exchange information with businesses. Where the Agency does collect consumer personal information, it should be required by Agency policy to implement and document appropriate technical and organizational measures to protect the data, including ensure that it deletes the data when no longer needed for an Agency purpose.

Companies should receive at least 30 days' notice prior to an audit. This is because businesses (particularly smaller ones) will need to redirect internal resources to respond to and support audit requests. It is also important to note that these audit do not relate to time-sensitive issues like workplace safety, pipeline safety, or some other activity where audit violations could result in death or injury.

The regulations should explicitly exempt attorney-client privileged material from the scope of audits, provide businesses with a reasonable timeframe to produce requested information, and comport with confidentiality requirements established under Government Code 11180 et seq.

CGA appreciates the opportunity to comment to the proposed language. We look forward to working with you on the implementation of these rules.

Sincerely,

[redacted]

Leticia Garcia
Director, State Government Affairs
California Grocers Association

From: Haley Cook [redacted]
Sent: 11/8/2021 4:30:15 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21: CrowdStrike Response
Attachments: 2021_11_8_CPPA.pdf; smime.p7s

[EXTERNAL]: prvs=7947b6631a=[redacted]

Hello,

Please find attached CrowdStrike's response to the CPPA's invitation for preliminary comments on the CPRA. Thank you.

Sincerely,

Haley Cook

Haley Cook
Associate Privacy Counsel
[redacted]

CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

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

8 November, 2021

I. INTRODUCTION

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), CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

The California Privacy Protection Agency (hereinafter "Agency") has written a thoughtful initial set of regulations. While we do not have feedback on every aspect, we do want to offer several points that may be of value to the Agency as it continues the rulemaking process.

A. Audits

i. General Commentary

When considering the requirements for the proposed audit and assessment requirements, especially regarding the the strictness of such requirements, it is important to consider that under CCPA, and soon CPRA, each of the parties (i.e.,

businesses, service providers, etc.), are contractually bound to those with whom there is privity of contract, and the resulting legal protections create a "Chain of Contractual Accountability." Moreover, each party must abide by its own CPRA requirements in a "Chain of Independent Obligations." In other words, consumer rights are protected by (i) enforceable contractual obligations between respective parties, including potential ad hoc audit commitments, and (ii) direct application of the CPRA to any party processing personal information within the scope of the law. This means that where both the Chain of Contractual Accountability and the Chain of Independent Obligations exist, strong accountability measures exist for CPRA compliance, with well-defined cybersecurity requirements further strengthening consumer data protection.

ii. Cybersecurity Audits

Today, data breaches pose some of the most significant threats to consumer privacy. This means that incentivizing the adoption of effective cybersecurity practices and technologies is paramount to achieving the CPRA's aims. To reach the goal of setting clear expectations, as well as defending a complex enterprise, CrowdStrike recommends establishing a uniform, high-level standard of cybersecurity.[1] Separate standards will result in unintended short-term and long-term consequences. In the short term, different rules and standards will yield divergent results, complicate security training, negatively impact the use of shared resources and services, and complicate collaboration between organizations and agencies. In the long term, independently-developed approaches will lead to confusion with respect to emerging security controls and updates to best practices. Consequently, this increases the risk of cybersecurity incidents. As such, cybersecurity audits should test compliance against established standards recognized by the Agency as most appropriate, whether that be NIST, ISO, or another widely-used standard.

More broadly, the adoption of principles-based cybersecurity requirements can incentivize both innovation and organizational implementation of state-of-the-art technologies to protect data. While the current legislative landscape is already influencing organizations to treat security breaches seriously, there are additional

[1] We understand that different standards may be appropriate based on the size of the business.

steps that can encourage proactive adoption of cutting-edge technologies, such as software-as-a-service (SaaS) solutions, from around the globe. The European Union General Data Protection Regulation (GDPR), for example, requires organizations to look to the "state of the art" and protect personal data with technological and organizational safeguards "appropriate to the risk." Creating non-prescriptive mandates that nonetheless encourage organizations to analyze the probability and severity of threats in line with technological realities is important for ensuring cybersecurity evolves with critical technologies.

iii. Risk Assessments

Risk assessments are distinct from audits and should not be standards-driven. The fundamental question of a risk assessment is "how effectively does the security program address the cyber risks the organization faces?" Flexible frameworks are ideal for this type of evaluation. The best risk assessments should combine the types of security measures but place them in an operational context—both in terms of what threat actors are likely to exploit and what defenders can realistically accomplish.

Risk assessments should be performed at a cadence appropriate to strike the right balance between consumer protection and compliance costs. Risk assessments conducted and filed with the Agency on a yearly basis may become resource-intensive and burdensome for the Agency and businesses, resulting in perfunctory reviews that do not effectively assess the risks to consumers. Internally, a business should conduct periodic risk assessments that considers how their security program stacks up against the risks they face. Further, businesses should conduct periodic exercises (annually or biennially) to test and strengthen their ability to respond to security incidents.

B. Automated Decision-Making

The widening adoption of Artificial Intelligence (AI)/Machine Learning (ML) periodically raises fears about automated decision-making, surveillance, algorithmic bias, and other negative externalities. In specific instances, these concerns may warrant evaluation or scrutiny. However, it is critical for policy makers to understand that AI/ML also has the opportunity to drive positive social

outcomes; is already widely deployed in important instances driving such outcomes; and creates the opportunity for innovation in a variety of important spheres, including industries such as medicine and education.

Our particular focus is on the use of AI/ML within cybersecurity solutions. Legacy cybersecurity solutions relied on scanning files against signatures of previously identified malicious files. This process was onerous, resource-intensive, and could be easily circumvented through the use of novel or slightly modified approaches. Next-generation solutions, which leverage AI/ML, can detect previously unknown threats based on their characteristics or behaviors. This offers much more robust protection against threat activity.

Leveraging AI/ML can achieve success against unknown unknowns. For example, a machine learning model, shipped to CrowdStrike's Falcon Platform customers in September 2019, detected with high confidence the SUNSPOT malware, which was central to a sophisticated campaign that targeted high-value government organizations in late 2020-early 2021.[2] This is one of many instances of AI/ML typifying the best ways to defeat threat actors using new or tailored tools, tactics, techniques, or procedures.

In cybersecurity, AI is an advantage, especially when added to enterprise security solutions, such as for many of the entities processing a significant amount of California consumers' data.[3] Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. By way of example, with the help of AI, CrowdStrike can stop an attack in its tracks because such technology works faster than conventional signature-based or indicator of compromise (IOC)-based prevention.

---

[2] Sven Krasser, "Stellar Performances: How CrowdStrike Machine Learning Handles the SUNSPOT Malware," CrowdStrike Blog (Jan. 21, 2021) https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/.

[3] Michael Sentonas, *How Artificial Intelligence is Becoming a Key Weapon in the Cybersecurity War*, CrowdStrike Blog, Oct. 24, 2017, https://www.crowdstrike.com/blog/how-artificial-intelligence-is-becoming-a-key-weapon-in-the-cybersecurity-war/.

We recommend that as the Agency continues to modernize privacy regulations, it keeps flexibility in mind. By this, we mean to emphasize the flexibility of AI as a positive tool in various situations, and not simply a technology regulated through the lens of an automated-decision making system that could harm California consumers.

We understand that the concern with AI is the possible harm to consumers, but for AI, like for any other technology, the context in which it is used, rather than the mere fact that it is incorporated, is material. Consequently, creating and relying upon a right to object to a particular technology or data processing methodology is not the best approach to protect rights in an ever-evolving technological landscape. Instead, we recommend protecting the rights of California citizens through a technology-neutral approach. When creating regulations on the safe use of AI, the Agency should consider adopting language similar to the General Data Protection Regulation's ("GDPR") requirement that organizations implement safeguards "appropriate" to the risk to protect personal information. This approach incentivizes organizations to take into account modern, rapidly-evolving data breach risks posed by cybersecurity threats from e-crime, 'hacktivist', and nation state actors using tactics such as ransomware, supply chain attacks, or malware-less intrusions.

III. CONCLUSION

The Agency's proposed regulations provide a thoughtful analysis of a complex legal and policy area. As updates to the law and administrative rulemaking moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the

ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Haley Cook
Associate Privacy Counsel

Email: policy@crowdstrike.com

***

From: Alastair Mactaggart [redacted]
Sent: 11/8/2021 4:03:07 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: 'James Harrison [redacted]' [redacted]; Rick Arney [redacted]
Subject: PRO 01-21 comment [Californians for Consumer Privacy comments on proposed regulations]
Attachments: CCP Letter to CPPA on proposed regulations 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 accept the attached comments on your rulemaking.

Yours sincerely
Alastair Mactaggart

Alastair Mactaggart, Chair
Californians for Consumer Privacy
1020 16th Street
Suite #31
Sacramento CA 95814
[redacted]

CALIFORNIANS FOR CONSUMER PRIVACY

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

Dear Commissioners and Executive Director Soltani:

Please find our comments with respect to your September 22, 2021 Invitation. We have interspersed excerpts from your document for ease of organization.

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

Cal Civ Code 1798.185(a)(15) was included in the California Privacy Rights Act ("CPRA") intentionally without specifying hard and fast guidelines constraining the California Privacy Protection Agency ("CPPA," or "the Agency"), in order to provide maximum flexibility to the Agency to select criteria for cybersecurity audits and risk assessments.

Our recommendation is that cybersecurity audits and risk assessments initially be applied to the largest personal information processors in California, and over time, to smaller ones.

For example it could make sense to limit this rule's application, initially, to businesses that:

- Collect personal information of more than 250,000 consumers.
- Collect sensitive personal information [§1798.140 (ae)], especially including children's information.

California voters saw fit to create a new category of "sensitive personal information," ("SPI") and CPRA requires such SPI be treated differently and more carefully than other personal information. By definition, any processing of such SPI presents a 'significant risk to consumers' privacy or security,' and therefore any entity processing SPI should be required to participate in the security audits and risk assessments.

The suggestion with respect to including processors who collect personal information ("PI") from 250,000 or more consumers is meant to allow the CPPA to fine-tune the audit and risk assessment requirements on a smaller group of processors, before expanding the requirement.

Annual Cybersecurity Audits

Initially, we feel that cybersecurity audits should score businesses against the Recommendations in the California Data Breach Report 2012-2015 issued February 2016 by Kamala Harris, CA Attorney General ("AG Recommendations").

There are 5 AG Recommendations, and the first refers to the Center for Internet Security's 20 Critical Security Controls, (now 18 CIS Critical Security Controls).

Meeting these recommendations should be the minimum threshold to demonstrate that a business' processing of PI does not present a "significant risk to consumers' privacy or security;" and should be a minimum requirement to demonstrate that a business has "reasonable security procedures and practices" as required in §1798.150(a)(1).

Additionally, consideration should be given to harmonizing CPPA's audit requirements with GDPR requirements, such as by considering including the ISO/IEC 27001 standards in evaluations of organizations' security procedures.

Regular Risk Assessments

We suggest that the timing for such risk assessments be linked to the intensity of PI and SPI processing: an organization processing large volumes of SPI, or that collects children's information, must report at least annually.

We also believe reports should be filed within a much shorter time period in the case of any significant change of procedure affecting consumers' privacy and security.

There is ample precedent for such a requirement in California. For example large oil refiners are required to monitor certain chemical compounds on a real-time basis, to ensure that in the event of any detrimental change, Californians can take steps to protect themselves. Large processors of PI and SPI should be required to inform the CPPA within a short time period when a change to their previously-submitted procedures risks diminishing consumer privacy and security.

In terms of coverage, we suggest considering harmonizing the risk assessments with GDPR requirements, such as the GDPR Data Protection Impact Assessment (see a suggested template here). Over time, the CPPA's focus should be on introducing regulations that encourage organizations to minimize the processing of PI, and its retention, and to maximize its security.

In conclusion, we emphasize that CPRA did not include an external standard or benchmark for either cybersecurity audits or risk assessments. This is by design, as we felt it critical that the CPPA has the flexibility to adopt different standards over time, in this rapidly changing area of technology.

2. Automated Decisionmaking

§1749.185(a)(16) is one of the most powerful clauses in CPRA, which we believe should and will eventually touch almost all aspects of online (and in some cases, offline) life in California.

As much as any part of CPRA, we feel this rule must evolve over time as business processes evolve, and as such we urge the Agency to approach this responsibility incrementally.

Our first suggestion is to address behavioral advertising, because at the most fundamental level, all behavioral advertising involves automated decsionmaking and profiling.

Algorithms that drive behavioral advertising rely on data about consumers, i.e. a consumer 'profile' assembled from that data; and rely on fraction-of-a-second decisions whilst interacting with either outside bidders (other advertisers) or a platform's own data and advertisers, to decide which ad to show a consumer.

As soon as a business assembles longitudinal, cross-platform/cross-site data about a consumer, it is engaging in profiling that consumer, and all advertising exchanges rely on algorithmic decisionmaking.

Consumers should be able to follow the logic involved in their interaction with a business, and if they see a particular ad, should be able to find out why they are seeing that ad. We urge the regulations to focus on granularity, and thus rather than a bland "you are seeing this ad because we have identified that you are interested in this subject matter," which accomplishes exactly nothing, we think it far more beneficial to consumers if they could discover that they are seeing an ad because they read an article or visited a website (i.e., "you are seeing this gay-directed ad on Facebook because you 'liked' Lady Gaga"), and then have the right to opt-out of such automated decisionmaking and profiling.

We emphasize behavioral advertising, since that is at the core of the surveillance economy, but clearly any businesses that rely on profiles or automated decisionmaking to respond individually to any consumer interaction or request, are also covered by this rule.

Ultimately, we suggest examining this new right in light of GDPR Article 13 (2)(f) and 14 (2)(g) (both referencing GDPR Article 22). While not identical in terms of consumer rights, the CPRA concept of 'meaningful information about the logic involved' in automated decisionmaking is drawn from the GDPR, and care should be taken to evaluate GDPR guidelines when promulgating regulations in this area.

In conclusion, we feel it important for the Agency to:

1) Pass regulations specifying that all behavioral advertising involves profiling and automated decisionmaking;
2) Clarify that 'meaningful information' in the context of behavioral advertising, means (to quote from the GDPR Guidelines) "the controller [should] provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full

algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for [the decision, which might be seeing an ad]."

3) Specify that consumers have the right to opt-out of this automated decisionmaking, and profiling, (which is the other side of the same coin as telling businesses not to sell the consumer's PI, or to use their SPI). By limiting, initially, the automated decisionmaking and profiling rules' opt-out provisions to cross-context behavioral advertising, the scope of this rule will be easy to understand, and this mandate is well-supported throughout the text of CPRA.

Subsequently, the Agency *should* extend this regulation and consumers' opt-out rights, to other areas of online and business activities, but we suggest that addressing the online advertising ecosystem will cover the biggest area where profiling and automated decisionmaking intersect with consumers' lives currently.

3. Audits Performed by the Agency

CPRA establishes a new position in California state government, a California Chief Privacy Auditor.

The language in §1798.185(a)(18) is intentionally broad, allowing the Agency to adjust requirements over time, and in response to changing business compliance, and consumer priorities.

The Auditor has the power to compel businesses to reply to the Auditor's requests for information, and the Auditor's scope should only be limited by whether a request is reasonably linked to a potential violation of CPRA.

We suggest the Agency not determine which criteria it will use to select businesses to audit (which because of open-meeting laws, would result in the publicization of same), but let the Auditor, in consultation with the Executive Director, determine such criteria. Announcing a limitation on the universe of companies to be audited serves no purpose other than to notify certain businesses that they are at a lesser or no risk for being audited, which in no way would improve consumer privacy or security.

With respect to safeguarding consumers' PI from disclosure to the Chief Privacy Auditor:

1) Note that §1798.185(a)(18) refers to 'protect[ing] consumers' personal information from disclosure to an auditor,' and there are two possible scenarios that fulfill this description: a business hires 'an auditor' to perform the cybersecurity audits and risk assessments set forth in §1798.185(a)(15); and then also when 'an auditor' on the Chief Privacy Auditor's staff is seeking information from a business.
   a) In the former case, the scope of the audit must ensure that PI and SPI is never turned over to the auditor, and the auditor should certify same.
   b) In the second case, pursuant to Civil Code section 1798.199.65, the CPPA auditor will have access to such information, the misuse of which would violate state law. (See. Gov. Code § 19990).

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

CPRA's new right for consumers to correct their information is especially important in light of the increasing trend for businesses to determine important outcomes in consumers' everyday lives, often without the consumer interacting with any live person at the business.

What jobs you're offered, what apartments you're shown, which schools may admit you, depend in many respects on what information businesses hold about you. And while these are very important areas of life, even seemingly less-important areas can be very consequential. It may seem amusing to read the link above (where Facebook deemed a user gay who had liked Lady Gaga), but if others in a person's life finds out that Facebook thinks them gay, the algorithm could have just made a life and death assessment.

The regulations envisaged in §1798.185(a)(8) should address the following:

1) A consumer should be able to request a correction for information which, if left uncorrected, would have a potentially significant impact on their lives. We think at a minimum, this should include all erroneous Sensitive Personal Information, i.e., if a business has incorrect SPI about a consumer, the consumer should always be able to request its correction.
2) By contrast, if a consumer is trying to play 'gotcha' with a business, and for example signed a liability waiver as "Mickey Mouse" prior to getting on a ride at a theme park, that would not reach the same threshold.
3) Equally, if a consumer determines that a three-year old browsing history includes visiting a website the consumer has no memory of having visited, or searching for a term they do not recall searching for, then the threshold for 'correcting' that information could be a) much less frequent, and b) non-existent in truly trivial cases, especially if the consumer has no proof.
4) Because all requests for correction are verifiable consumer requests, per §1798.106(c), there is no more of a vector for fraud with respect to correction requests than there is for access or deletion requests, so the only provisions to be taken with respect to preventing fraud in §1798.185(a)(8)(C) is to ensure that all correction requests remain verifiable consumer requests. The regulations should ensure no additional barriers are erected by businesses (not simply with respect to correction requests, but also for access and deletion) to prevent consumers using their new right to correct their information.
5) "Impossibility," and "disproportionate effort" in §1798.185(a)(8)(A) were included to address items where it was literally almost physically impossible or extraordinarily difficult to correct an item, for example if a consumer were to allege without any proof that they had visited a website, many years ago—that type of thing, almost a frivolous request.
6) The insert with respect to the written addendum in §1798.185(a)(8)(D) was included largely as a result of the not-uncommon experience of some health care providers, who are forced by law and medical ethics to include an incident on a patient's chart, which the patient wishes not to be included on the chart. One can imagine a consumer wishing to expunge anything from a psychotic episode, to self-harm, to a drug or alcohol relapse, and a hospital or medical practice being unable to simply 'correct' that episode by saying it never happened.

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

CPRA improves on CCPA's consumer rights with respect to the propagation of consumer PI and SPI in the ad-based surveillance economy in two major ways.

First, it clarifies and reinforces that "Sale" as defined in CCPA, means 'including when a business shares personal information and tries to play a game to get around the definition of 'sale' by pretending it's not a 'sale' of information.'

With the passage of CPRA, it is now crystal clear in statute that when a consumer clicks "Do not sell or share my Personal Information," the consumer means a) do not sell my information, and b) do not share it with another company for the purposes of cross-context behavior advertising.

In essence, when the consumer clicks the "Do not sell or share my Personal Information" button, they are eliminating the entire universe of possibilities for their current interaction ever serving as the basis for any future ad, *other than* a) as a target for a real-time, contextual ad then and there, and b) as part of data assembled *by the website the consumer is "intentionally interacting" with at that moment,* for use by that site, *on that site,* in the future.

Here are important points that the regulations should address:

CCPA Regulations—Suggested Corrections to Existing Regulations

1) The "Do not sell or share my Personal Information" button is supposed to be on *every page* that collects personal information. §1798.135(a)(1) clearly requires that the business "Provide a clear and conspicuous link ***on the business's internet homepages***, titled "Do not sell or share my Personal Information…." [bold italics added]
   a) Please note that the word in statute is 'hompages' not 'homepage.' This is intentional.
   b) "Homepage" is clearly defined as "***any*** internet web page where personal information is collected."
   c) However CCPA Regulation §999.306(b)(1) suggests the business is allowed to post the "Do Not Sell My Personal Information" link 'on the website **homepage"**
      i) This regulation must be clarified by including the word from the statute, "homepages," [i.e. the plural], as the inclusion of the plural word in §1798.135(a)(1) was meant to encompass **every page** that collects consumer PI.
   d) The rational for this is clear: if every page that collects consumer PI has a simple and clear "Do Not Sell My Personal Information" [and under CPRA, "Do Not Sell or Share My Personal Information"], then firstly, the consumer will be more aware of the practice in general, and secondly, businesses will have more incentive to stop selling/sharing PI, as they will not wish to devote a material part of every webpage on every mobile screen, to this button.
      i) This negative incentive is a ***critical*** part of both CCPA and CPRA, and by ignoring this architecture, the regulations have woefully undercut the reach of CCPA. We urge the Agency to correct this error when the CPRA regulations are promulgated.

2) In addition, the CCPA regulations have massively weakened the statutory intent of CCPA by introducing a 15-day period to comply with opt-out requests by consumers:
   a) Regulation §999.315(e) states: *"A business shall comply with a request to opt-out as soon as feasibly possible**, but no later than 15 business days from the date the business receives the request.** If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information." [Bold added]*
   b) The statute makes no mention of any delay, and instead of over two weeks, implies immediacy. CCPA §1798.135(a)(4) states "For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer." <u>There is no fifteen-day period to comply</u>.
   c) It is incomprehensible that the regulators would include this language "*If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request.*". This is a regulatory *gift* to the advertising industry, and the absurd result is that as soon as a consumer visits a website, a business can begin selling the consumer's personal information, often within less than a second; but if the consumer opts out of the sale of their data, the business can *keep on selling* that information for more than 2 weeks.
      i) We believe this 15-day period would absolutely violate the direction in §1798.185(a)(4)(A) that consumers obtain "the ability to exercise their choices *without undue burden*…" 15 days is absolutely an undue burden for consumers who seek to have the spread of their information limited.
   d) We understand that for certain offline use cases, a direction not to sell PI could take longer; but in an online, digital world, if the switch to sell personal information can be turned on instantaneously (which it can be and is); then it should be able to be turned off instantaneously (and not half a month after the consumer has directed!).

<u>CPRA Regulations (new)</u>

1) Regulations established pursuant to CPRA 1798.185(a)(4)(A) should, with respect to the mandate to "prevent businesses from engaging in deceptive or harassing conduct," reference the powerful language in CPRA 1789.121(a) limiting use of consumer SPI to "perform[ing] the services or provid[ing] the goods reasonably expected by an average consumer."
   a) We would urge the Agency not to get too prescriptive in this section, as we believe general language will allow for greater flexibility in enforcement.
2) Regulations established pursuant to 1798.185(a)(19) should make clear that this paragraph (19) covers *all* the opt-out references in CPRA.
   a) Note that while 1798.135(b)(1) references 1798.185(a)(20), not (19), that is because (20) deals with constraints on a business' *response* to an opt-out/SPI limitation request received from a consumer.
   b) The actual mechanics of how the signal is constructed, are delineated in paragraph (19).
   c) The most important message here is that consumers must be able to "set it and forget it." If privacy rights are difficult to access, then consumers will not avail themselves of them.

Consumers ***must*** be able to set their browsers, devices and apps to a 'maximum privacy' setting and then proceed without thinking any more about the subject, and the law should then protect them to the maximum extent possible.

3) On this topic, 1798.185(a)(19)(vi)(a) ensures that the signal may have a 'most restrictive' setting, which enables a consumer to easily select the most privacy-protective setting for their browser, app, or device. While (b) and (c) of this same subsection do allow for other, less privacy-protective settings, we expect that the vast majority of privacy-minded consumers will select the first setting.
   a) Note also that while 1798.185(a)(19)(A)(iii) states the signal must "clearly represent a consumer's intent and be free of defaults…presupposing that intent," there is absolutely no wording in the statute that would prevent a privacy-focused business from highlighting (19)(vi)(a) as *the* choice most consumers *should* select if they want maximum privacy. Education by a business on this point would actually ensure that a consumer's intent was clear. The statute intentionally allows a business to explain to a consumer that they should select (19)(vi)(a) if they want the maximum privacy protection.
4) Also, 1798.185(a)(19)(C)(iv) covers an important aspect of the SPI use limitation included in 1798.121(d):
   a) The issue is that some SPI is not treated by businesses as SPI. Think of a security camera monitoring a shopping mall: everyone's face is SPI, except if the security system doesn't use facial recognition on the video data, then the system isn't collecting that SPI for "…the purpose of inferring characteristics about a consumer…"
   b) However, to ensure that this exception in 121(d) is not used as a loophole, 1798.185(a)(19)(C)(iv) was inserted to allow regulations to exclude this fact set.
5) Age limitation: we believe parents of children (or the children themselves) should be able to clearly set a device, browser or app to specify that the user is less than 13, or is between 13 and 16.
   a) This should be a simple setting, and easy to enable.
   b) There must be tremendous focus on the setting being secure, i.e. that a third-party cannot manipulate the signal to turn it off surreptitiously.
   c) We do not see that this ever requires the disclosure of children's information to businesses. We think an accountholder should be able to enact the control, and there should be safeguards to prevent a minor from disabling the control except with the consent of the accountholder.
   d) There are ample examples of this mechanism in use today; for example the Apple ecosystem has effective parental controls.
   e) Regulations should specify that businesses that do not subsequently respect the age-specific signal, are in intentional violation of CPRA.
6) Finally, with respect to the "opt back in" mechanism delineated in 1798.185(a)(20)(C): this section was included because in the event a consumer wants to opt back in to having their data sold or shared, they should be able to; but, importantly, businesses must not be able to use this link to trick consumers into opting back in.
   a) Note that any such opt-in must only apply to the business with which the consumer is intentionally interacting. This is important, given GDPR experiences where Business A required Business B to obtain opt-in permission from consumers, and held that a consumer's opt-in to Business B, was valid for Business A (even though the consumer only understood they were interacting with Business B).

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

1) With respect to SPI "collected or processed without the purpose of inferring characteristics about a consumer," please see the comments in answer 4) immediately above.
    a) Example: a consumer rides in a shared car. While in the car, they leave biometric information (hair, skin cells), but while such information is clearly SPI, and is 'collected' in the vehicle, the ridesharing business is not collecting/processing the information "for the purpose of inferring characteristics about a consumer."
        i) Clearly, if the business *were* to start collecting iris-prints or fingerprints from its customers in order to identify them, then that would be a collection of SPI that squarely fell within the protections granted consumers by 1798.121, and would not qualify for the 121(d) exemption.
2) With respect to what use of SPI should be allowable notwithstanding a consumer's direction to limit its use, those uses are limited at this time *only* to those matters specified in 1798.140(e)(2),(4),(5) and (8), or that an average consumer would expect who had requested the goods or services.
    a) Importantly, none of these uses cover any behavioral advertising whatsoever (but for example, a website discussing cancer treatments could show a non-specific, contextual ad for a cancer center).
3) We believe the 'reasonably expected' limitation should be construed as a 'necessary in order to provide' test.
    a) For example, a ridesharing business *does* need to know a consumer's exact location to deliver a vehicle to them. It is not practical for a consumer to instruct a business not to use that SPI, *and* at the same time require the business to deliver them the service.
    b) Or, a health monitoring wearable device *does* need to use the consumer's biometric data to deliver the product the consumer has requested (on the other hand, this reasonable expectation does *not* extend to the business then selling or sharing that SPI).
4) In the future, the Agency could expand the list of allowable uses beyond those allowed now.

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

We believe that information that has already been deleted by a business will be impossible to provide back to consumers in response to an access request. CPRA was designed partially to give businesses incentives to move towards privacy-by-design. If a business does not have to produce information, because it has deleted that information (and therefore can no longer use it), that is overall a good outcome, in our view.

8. Definitions and Categories

1) We believe that at this time, the Agency should expend its efforts in creating regulations around the existing definitions of 'personal information,' 'sensitive personal information,' 'deidentified,' 'unique identifier,' which we believe are adequate at this time and for this round of rulemaking.
2) With respect to 'designated methods for submitting requests,' we believe existing CCPA regulation §999.315 should be amended as follows:

a) §999.315(c) states that businesses "...shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device 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 submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer."
   i) However, there is literally no mention of this mechanism at all in CCPA §1798.120, and the Regulations seemingly invent this requirement for businesses to honor a browser, device setting etc., out of thin air, when they reference this section.

b) The regulations should, in fact, have referenced a *different* section of CCPA, i.e. CCPA §1798.135(c), which specifies that "[a] consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, 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."
   i) A browser, application setting or device setting qualifies as "another person" pursuant to the definition of "person" in CCPA §1798.140(n). In fact, this concept is one of the cornerstones of CCPA—the notion that consumers **must** be able to exercise their privacy choices through another party.

c) Importantly, CCPA distinguishes between privacy choices, and takes a different approach when fraud poses a security risk (think Alice pretending to be Bob for an access or deletion request) by requiring a verifiable consumer request. However, opting out of the sale of personal information was specifically designed to involve a much lower threshold, requiring merely an "authorized request" from a consumer, since there is no negative security implication involved in Alice pretending to be Bob, and opting out of the sale of his information.

d) To conclude, we believe CCPA regulation §999.315(f) misreads the existing statutory language in CCPA §1798.135(c).
   i) First, we urge the Agency to do away with the requirement that consumers provide authorized agents "written permission signed by the consumer." There is nothing in the statute requiring "written permission signed by the consumer," and on the contrary, the threshold for authorizing "a person" to opt out on the consumer's behalf was deliberately set lower than that for access or deletion requests.
      (1) A browser or device set to "do not sell," should be all the evidence necessary to a business, that the inbound signal from a consumer, must be treated as a do-not-sell/share signal.
   ii) Second, we disagree entirely with the second half of §999.315(f), which states that "[u]ser-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information *shall be considered a request directly from the consumer,* not through an authorized agent."[italics added] While we understand the intent, the precedent this sets is misguided as it misinterprets and ignores the clear statutory intent of §1798.135(c).

iii) We believe the regulations should clearly state that user-enabled privacy controls ***are*** requests from "a person authorized by the consumer to act on the person's behalf;" and as such, ***must*** be treated by businesses as a request from the consumer's authorized agent that must be complied with, as set forth in §1798.135(c). The "shall be considered" language in the statute implies that the Regulator is doing consumers a favor by broadening the reach of CCPA, whereas the Regulator has an ample statutory intent to prove that opt-out signals from browsers, devices and applications must be treated as coming directly from a consumer.

iv) This may seem a lot of verbiage to spend on a point that ultimately should achieve the same goal, but we think the current Regulations are built on the wrong foundation. CCPA provides a strong framework for global privacy settings, user-enabled controls, and device settings to act to protect consumers' privacy, and we think relying on the statute, as opposed to the AG's interpretation, will better insulate the regulations from any challenge.

3) With respect to further defining the business purposes for which businesses, service providers, and contractors may combine consumers' personal information that was obtained from different sources:
   a) We think it important to note that the governing language in CPRA §1798.185(a)(10) provides that any expansion of the term "business purposes" must be "consistent with consumers' expectations." Note, this should not be interpreted as a one-way street only, ie in the direction of *expanding* "business purposes." For example, "...further defining and adding to the business purposes..." could include regulations which *narrow the scope of existing business purposes,* which would qualify as a "further defini[tion]" of business purposes.
   b) In addition, the second half of paragraph (10) has the same framework. The language "further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources" can and may involve the Agency *narrowing* the permitted uses for which such combinations can be used.
   c) Finally, we urge the Agency to consider both CPRA §1798.185(a)(10) and CPRA §1798.185(a)(11) in tandem, as both govern the scope of "business purposes," which is such a key area of the law. CPRA's clear intention in §1798.185(a)(11) is that all business purposes "maximiz[e] consumer privacy." That is the test which regulations affecting "business purposes" must meet.
4) We believe the definitions of "intentionally interacts," "precise geolocation," "specific pieces of information obtained from the consumer," are satisfactory at this time as written.
5) We believe that further definitions of the term "law enforcement agency-approved investigation" can wait, as the requirement in §1798.145(a)(2) includes having an active case number, which precludes the 'rogue agent' scenario that always causes concern in these situations, and requires multiple approvals and visibility into initiating such an investigation.
6) We believe that the definition of "dark patterns" does not need to be addressed or updated at this time.

9. Additional Comments
Please provide any additional comments you may have in relation to the Agency's initial rulemaking

Based on the amount of misinformation we have seen from the advertising and technology industries in the year since CPRA passed, we thought it vital to clarify one of the most important parts of CPRA, namely the mechanism around opt-out, the opt-out button, and CPRA §1798.135 in general.

Many have suggested the CPRA makes an opt-out button optional. This is categorically untrue. Many have suggested that CPRA allows for businesses to ignore opt-out signals received from authorized agents. This is also untrue.

CPRA requires <u>all</u> businesses to honor global opt-out / electronic opt-out signal sent by a browser, application or device.

CPRA §1798.135 (e) states that "A consumer may authorize *another person* to opt-out of the sale or sharing of the consumer's personal information…*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." [Italics added]

Clearly, 1798.135(e) allows for a *person* to do the opting-out on the consumer's behalf [see definition of 'person' in §1798.140(u)]. There is no reading of the statute that would allow a business to refulse to honor a global opt-out signal enabled by a consumer.

CPRA requires businesses either to have "Do Not Sell/Share/Limit Use of SPI" button; or, to honor opt-out signals *with no retaliation or negative action taken by the business* in response to receipt of signal. The optionality is whether the business can retaliate against a consumer who opts out, not whether the business has to honor the opt out in the first place.

§1798.135(b)(1) reads "… 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*…" [italics added]

Then, §1798.185(a)(20)(B) constrains the business from responding by altering the functionality, charging the consumer a fee, including a pop-up, etc., in response to the consumer's instruction to opt-out of the sale of their information--essentially it takes the list allowed by 1798.125 delineating what a business can do in response to an opt-out signal, and negates it.

The flow chart is as follows:

1798.135(b)(3) Business chooses whether to comply with 1798.135(a) or (b)

1798.135 (a) Business must display DNS/DNS link on **all** homepages, but retains ability to charge a fee, change terms etc. for consumers who opt-out, per §1798.125

1798.135(b)(1) Business can not display Do Not Sell/ Do Not Share link, but now it MUST:

Not avail itself of any 1798.125 permitted retaliations [see 1798.185(a)(20)], which essentially prohibits all actions that would be allowed pursuant to 1798.125.

Note: while 1798.135(b)(1) does not specifically mention 1798.125, it states the opt-out signal must comply with 1798.185(a)(20), and so the effect is that no business choosing the 1798.135(b)(1) route is permitted to do anything other than opt the consumer out. 1798.185(a)(20) prohibits all the actions that 1798.125 would have allowed. In essence, if a business chooses not to have the Do Not Sell / Do Not Share button, it cannot avail itself of any allowed responses in 1798.125, nor can it pop up a notice, etc.

§1798.135(e) merely reinforces, for the sake of emphasis, that a business *must* always comply with a DNS/DNS signal sent by another person (ie browser etc).

Conclusion: either businesses post a DNS/DNS/limit SPI link or button on *all* pages that collect PI, and retain the ability to differentiate their treatment of opting-out consumers; or, they don't have that link, but then they must seamlessly and with essentially zero negative impact to consumers, stop selling or sharing SPI, and limit the use of SPI, for consumers who opt out. If a consumer has their browser set to DNS/DNS, or the Global Privacy Control enabled, then any businesses opting to follow 1798.135(b) must silently comply with the request.

This is meant as an incentive—because while some businesses will want to keep selling PI, and want to make it difficult to opt out, we hope that the market will eventually reward those businesses that simply allow for an opt-out without any negative reaction to the consumer opting out.

One suggested regulation: allow consumers to verify somewhere on the site, that the consumer's instruction has been adhered to, and the business is not selling or sharing their PI, and is limiting the use of their SPI. We think a pro-active attestation by the business, will be comforting for consumers (i.e., "We are not selling your information or sharing it for cross-context behavioral advertising, as those terms are defined in the California Privacy Rights Act."

Congratulations to the commissioners and the Executive Director on your appointments. We look forward to working with you to craft effective regulations to implement this groundbreaking law, which will allow California to lead the entire U.S. towards greater consumer privacy.

Yours Sincerely

/s/ Alastair A. Mactaggart
Chair, Californians for Consumer Privacy

From: Tanya Forsheit [redacted]
Sent: 11/8/2021 3:44:18 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: Comments of the News Media Alliance in Response to the CPPA's Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020, PRO 01-21
Attachments: NMA CPRA Preliminary Rulemaking Comments 11821(21453327.1).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.

Attached please find the Comments of the News Media Alliance and California Newspaper Publishers 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, PRO 01-21.

Tanya Forsheit
Partner and Co-Chair, Privacy, Security & Data Innovations

10100 Santa Monica Blvd., Suite 2200 | Los Angeles, CA 90067
Direct Dial: [redacted] **Fax:** 310.282.2200 | **E-mail:** [redacted]
Los Angeles | New York | Chicago | Nashville | Washington, DC | San Francisco | Beijing | Hong Kong | www.loeb.com

Tanya Forsheit
Partner

LOEB & LOEB LLP

10100 Santa Monica Blvd., Suite 2200 | Los Angeles, CA 90067
Direct Dial: [redacted] | **Fax:** 310.282.2200 | **E-mail:** [redacted]
Los Angeles | New York | Chicago | Nashville | Washington, DC | San Francisco | Beijing | Hong Kong | www.loeb.com

November 8, 2021

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

Re: Comments of the News Media Alliance and California Newspaper Publishers 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, PRO 01-21

The protection of the free press is enshrined in the First Amendment to the U.S. Constitution. The free press is on the front lines helping the American people hold accountable those who hold positions of power within our democracy and around the world. A vibrant and financially stable independent press is therefore essential to a healthy democracy. The News Media Alliance (the "Alliance") represents over 2,000 media outlets and is composed of nationally recognized media organizations of all sizes ranging from international to hyperlocal.

Digital advertising is a significant source of revenue to media outlets, large and small, and sustains independent journalism by helping to keep the press affordable and free from government control. In the two-and-a-half years since the Alliance submitted comments to then Attorney General Xavier Becerra in connection with the rulemaking under the California Consumer Privacy Act ("CCPA"), journalism has become even more financially vulnerable and more reliant on digital ad revenue for its very existence. When Governor Brown signed the CCPA into law in 2018, digital advertising constituted 49% of journalistic media revenue. In 2020, that share rose to 63%.[1] And while digital revenue is making up a greater portion of total advertising revenue and total revenue, total estimated advertising revenue is actually down, by as much as 29% from 2019 to 2020 by some accounts.[2]

With a well-designed privacy law, the press can continue to do its job as intended in the U.S. Constitution, and consumers can continue to have access to cost-efficient news sources, as well as control of the use and exchange of their personal information. The regulations ("Regulations") to be promulgated by the newly constituted California Privacy Protection Agency ("CPPA") under the California Privacy Rights Act ("CPRA") will play a significant role in the governance of privacy practices in the digital advertising ecosystem, and provide guidance to other states as

[1] Pew Research Center on Journalism and Media available at https://www.pewresearch.org/journalism/chart/sotnm-digital-and-non-digital-advertising-revenue/

[2] Pew Research Center on Journalism and Media available at https://www.pewresearch.org/journalism/fact-sheet/newspapers/.

they consider their own legal framework.

The Alliance believes in giving consumers more transparency and control regarding the collection, use, and sharing of their personal information. The Alliance also supports clear and consistent rules that align with other privacy laws around the world and that support practical implementation and operationalization by news publishers of all sizes across digital and offline media, regardless of jurisdiction.

The Alliance, joined by the California Newspaper Publishers Association, respectfully submits the following comments on certain topics (designated below) as identified in the Agency's Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21) dated September 22, 2021.

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

The CPRA Regulations Should Align with Existing Privacy Laws, Including the GDPR, the VCDPA and the ColoPA.

Laws in Europe, and here in the U.S., have already outlined the circumstances in which a business' processing of personal information presents a "significant risk to consumers' privacy or security." As such, the Alliance recommends that the Regulations align with existing privacy laws on this issue, including the European Union General Data Protection Regulation ("GDPR")[3], the Virginia Consumer Data Protection Act ("VCDPA")[4], and the Colorado Privacy Act (ColoPA).[5] Such harmonization will provide much needed consistency and predictability as to when a covered business must perform cybersecurity audits and risk assessments with respect to their processing of personal information.

Under the GDPR, a Data Protection Impact Assessment ("DPIA") 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.

Similarly, under the VCDPA and the ColoPA, in order to present a significant risk to consumer's privacy, the profiling at issue must be made in furtherance of a decision by the controller that results in the provision or denial by the controller of: (i) financial and lending services, (ii) housing, (iii) insurance, (iv) education enrollment, (v) criminal justice, (vi) employment opportunities, (vii) health care services, or (viii) access to basic necessities, such as food and water (or, in the case of the ColoPA, access to "essential goods or services"[6]).

---

[3] GDPR Art. 35. *See also* "Guidelines on Data Protection Impact Assessment (DPIA)," available at https://ec.europa.eu/newsroom/article29/items/611236).

[4] Va. Code Ann. § 59.1-576.

[5] Colo. Rev. Stat. § 6-1-1301.

[6] Colo. Rev. Stat. § 6-1-1303(10).

The Alliance suggests that the Regulations should not require covered businesses under the CPRA to engage in the costly and burdensome task of submitting a risk assessment to the Agency unless the processing of personal information at issue rises to the level of "significant risk" identified in the GDPR, VCDPA, and ColoPA.

II. Topic 2: Automated Decisionmaking

The Rules Should Align with the GDPR and Should Appropriately Balance the Interests of Consumer Safety and Security with Those of Consumer Privacy.

The Agency is fortunate to be able to look to existing privacy law that describes the kinds of activities that should be deemed to constitute "automated decisionmaking technology" or "profiling." As such, the Alliance respectfully recommends that the Regulations should, wherever possible, align with the GDPR. Specifically, automated decisionmaking should be limited to decisions based *solely* on automated processing and which produce legal effects concerning a consumer or significantly affect a consumer in a similar way.[7]

Also consistent with the GDPR, the Regulations should allow for decisions based on automated processing or profiling (and limit a consumer's ability to opt out of such automated processing or profiling) where the processing is expressly authorized by law to which the business is subject, or necessary for entering into, or the performance of, a contract between the consumer and the business, and in situations where consumer safety could be endangered in the absence of such decisions (such as in the case of identity theft, and fraud monitoring and prevention).[8]

In addition, the Regulations regarding the kind of 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, should not require businesses to disclose trade secrets, confidential business information, or other information that might allow fraudsters or other bad actors making access requests to harm or jeopardize the security and safety of other consumers.

III. Topic 3: Audits Performed by the Agency

The Regulations Should Incorporate an Objective Standard for the Initiation of an Audit.

The Alliance respectfully recommends that the Regulations set forth an objective standard to guide the Agency's selection of which businesses it will audit and the Agency's determination of when an audit is necessary. In order to conserve scarce Agency resources, the Agency should initiate an audit when the Agency has evidence to support a reasonable belief that a violation of the CPRA has occurred. The scope of the audit should similarly be limited to the processing of personal information that gave rise to the purpose for initiating the audit. The Regulations should also include requirements for technical, administrative, and physical safeguards that the Agency must follow in order to protect consumers' personal information during the performance of the audit and to ensure that the audit is not unduly burdensome.

---

[7] GDPR Art. 22.

[8] GDPR Recital 71.

IV. Topic 4: Consumers' Right to Delete, Right to Correct, and Right to Know

A. Businesses Should Have 45 Days from the Date of a Request to Know or a Request to Delete is Verified to Fulfill or Deny that Request.

The Alliance respectfully recommends that the Regulations modestly modify the CCPA regulations in order to address operational complexities raised by existing verification requirements. The CCPA Regulations currently provide as follows:

> Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request.[9]

The experience of businesses addressing complex and multifaceted verification requirements under the CCPA, and the time that consumers take to respond to such requests for verification, supports a slight revision of this aspect of the CCPA regulations. The time required for verification should not count towards the total time allotted for the business to complete the request. The Alliance therefore recommends that the Regulations revise the CCPA regulations such that the 45-day window to respond to requests to delete and requests to know begins to run on the day the request is verified by the consumer.

B. The Rules Should be Consistent with the Existing CCPA Regulations.

There are a number of processes and standards put in place under the CCPA regulations that should remain consistent under the CPRA Regulations. For example, under the CCPA regulations, businesses may offer the consumers the option to delete select portions of their personal information as long as a global option to delete all personal information collected from them is also offered and more prominently presented than the other choices.[10] The CCPA regulations also provide that "a business may use a two-step process for online requests to delete, where the consumer must first submit the request to delete and then separately confirm that they want their personal information deleted."[11] Further, the existing CCPA regulations specify that a business may comply with a consumer's request to delete their personal information by de-identifying or aggregating the information.[12] The CCPA regulations also provide that, if a "business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose."[13]

---

[9] 11 CCR § 999.313(b).

[10] 11 CCR § 999.313(d)(8).

[11] 11 CCR § 999.312(d)

[12] 11 CCR § 999.313(d)(2).

[13] *Id.* (d)(3)

The Alliance recommends that these existing CCPA regulations remain in place under the CPRA in order to provide consistent and predictable guidance to, and save unnecessary expense and burden for, businesses that have expended time and effort putting CCPA compliance programs in place.

V. Topic 5: Consumers' Right to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of Their Sensitive Personal Information

The Regulations Should Allow for Technologically Appropriate Approaches to Opt Outs Across Channels, and Provide a Grace Period for Organizations to Implement All Necessary Opt-Out Mechanisms.

Publishers value their trusted first-party relationships with their readers. Therefore, news media have worked tirelessly over the last two years to put in place consumer-friendly links and backend systems to allow consumers to opt out of sale, as that term is defined under the CCPA. The CCPA itself made clear that a Do Not Sell My Personal Information link, on websites and in mobile apps, was the method by which businesses were required to provide this choice to consumers. Due to legacy technologies and platforms that often vary across different publications, news media have faced tremendous challenges in implementing such opt outs across properties and geographies, not to mention addressing situations where sales may occur offline. It is already impossible, from a technological perspective, for one single link on a web page to meet all of these needs.

The CPRA affords consumers new rights to opt out of sharing for cross-context behavioral advertising and to limit the processing of their sensitive personal information. The explicit language of the CPRA helpfully provides businesses with a choice to either provide links for a consumer to exercise these rights or "allow[] 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, … to the business indicating the consumer's intent to opt out of the business' sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both."[14] The Alliance supports Regulations that mirror this language in the statute.

No single opt-out preference signal, including the Global Privacy Control, can provide a one-stop-shop for consumers to opt out of all sales and sharing for cross-context behavioral advertising, much less to limit the use of sensitive personal information. The Alliance respectfully submits that the Regulations should not mandate the use of the Global Privacy Control or any other single opt-out preference signal.[15] Instead, the Alliance recommends that the Regulations support the use of

---

[14] Civil Code § 1798.135(b).

[15] The Global Privacy Control is not an "Easy Button." It does not work on all browsers, much less mobile operating systems or offline. In the event that the Agency promulgates Regulations that mandate the implementation of the Global Privacy Control, it should also mandate that all browsers adopt the Global Privacy Control so that consumers are not misled that use of the Global Privacy Control can opt them out of all third party ad tracking on all browsers. In such an event, the Agency should also explicitly provide guidance on how businesses are expected to provide opt-out rights on mobile platforms and offline, where the Global Privacy Control is not supported.

the Global Privacy Control or another opt-out preference signal, but also allow businesses to put in place as many different technologically appropriate and conspicuous methods as needed to provide all consumers (regardless of their authentication status) with robust opt-out choices across all browsers, media, devices, operating systems, and platforms, as well as with respect to offline "sales" such as list rentals.

Further, given these new consumer rights and the challenges of implementing opt-out requirements in a manner that will be honored by downstream ad tech players (that publishers do not control), the Alliance also respectfully requests that the Agency incorporate a compliance grace period for such implementation, up to and including January 1, 2025.

VI. Topics 6 (Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information), and 8(b) (the Definition of "Sensitive Personal Information")

The Regulations Should Allow for First-Party Targeted Advertising Based on Reader Interest in Sensitive Content

The CPRA statute is clear that there are certain limited but critical circumstances in which consumers cannot opt out of processing of sensitive information: specifically, when such information is used: (i) to "improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business";[16] (ii) to "provid[e] analytic services"[17]; or (iii) for "[s]hort-term, transient use, including, but not limited to, nonpersonalized 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."[18]

The Alliance respectfully requests that the Regulations align with the use cases described in the statute. In addition, the Alliance recommends that the Regulations support all forms of first-party advertising, even when such advertising is based on a reader's visit to an article regarding a sensitive topic. Publishers derive revenue (without which some outlets would not survive) by adding readers to aggregated demographic segments to which advertisements are targeted (such as "interested in medical articles"). Taking note of the fact that a consumer has read such an article does not equate with an inference that the reader has that sensitive condition at issue or is otherwise a member of group characterized by the sensitive condition. These segments are created based on whether a reader visited a particular article on a publisher's site regarding a sensitive topic. Such advertising is not based on the tracking of a device or an individual across sites or apps, and is limited to a single publisher's universe. Not only do many Alliance members heavily rely on such first-party advertising revenue but publishers also need the ability to use this first-party data (on a sensitive topic, or otherwise) to highlight or suggest similar content that the reader may be interested in (solely based on other articles the reader has viewed on the publisher's site). Without such an exception, medical news publications, for example, would not be able to use first-party data

---

[16] Civil Code § 1798.140(e)(8).

[17] *Id.* § 1798.140(e)(5).

[18] *Id.* §1798.140(e)(4).

to suggest other articles to a reader regarding similar symptoms or treatments. For both of these reasons, the Alliance recommends that the Regulations deem the use of information to create such segments for targeting as "collected or process[ed] without the purposes of inferring characteristics about a consumer" and therefore not subject to a consumer's right to limit use and disclosure of sensitive personal information. By contrast, the Alliance strongly supports Regulations that allow a consumer to limit the use of their sensitive personal information with respect to targeted advertising based on third-party tracking or sharing.

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

The Regulations Should be Consistent with the CCPA Regulations, and Should Provide a Reasonable Standard For the Provision of Information Beyond a 12 Month Window.

For security reasons, the Alliance strongly supports the Regulations remaining consistent with those of the CCPA such that they prohibit disclosure of sensitive information in response to consumer's requests to know.[19] This is particularly relevant since the CPRA covers employee data, as employers necessarily store sensitive information of employees, including social security numbers, health and benefits information, and financial information.

In addition, the Regulations should adopt a reasonable standard to govern a business' determination as to whether providing information beyond a 12-month window would involve a disproportionate amount of effort. Certain data sets (for example, unstructured data) would require a disproportionate amount of effort even to piece together whether data belongs to a certain consumer; impossible should not be the standard.

VIII. Topic 8 Definitions and Categories

A. Topic 8(e): The Business Purposes for Which Businesses, Service Providers, and Contractors May Combine Consumers' Personal Information that was Obtained from Different Sources

Businesses and Their Service Providers and Contractors Should be Allowed to Combine Personal Information from Different Sources for Consumer-Friendly Business Purposes

Businesses and their service providers and contractors should be able to combine personal information from different sources for legitimate business purposes. Under the current CCPA regulations, a "service provider" cannot build or modify household or consumer profiles to use in providing services to another business, or correct or augment data acquired from another source.[20] The Alliance submits that the Regulations should support these uses of data by service providers in ways that promote consumer privacy, even if that involves the combination of information from different sources and/or the use of information to provide services to more than one business.

---

[19] 11 CCR § 999.313(c)(4).

[20] 11 CCR § 999.314(c).

For example, the Regulations should support the combination of personal information from different sources:

- To enable businesses to better understand the demographic make-up of the communities they serve, for internal business planning/benchmarking purposes. For example, publishers obtain age and gender data from a vendor to compile general statistics about the demographics of event attendees (but do not use this information to create profiles or individually target those attendees).

- For purposes of data hygiene. For example, publishers may use a vendor to check public databases to make sure the publisher has up to date, accurate contact information (name, mailing address, phone number) for their subscribers/users for direct marketing purposes. Section 999.314(c) of the CCPA regulations should be revised to allow for this practice as a business purpose, as it is both privacy- and consumer-friendly.

B. Topic 8(j): Defining "Dark Patterns" The Regulations Should Align with Existing EU Standards for Obtaining Consent.

The Alliance maintains that it is critical that the Regulations include clear parameters of what is an acceptable method to obtain consent or to provide choice to a consumer, where required (e.g., for financial incentive programs). Accordingly, the Regulations should align with existing guidance from EU regulators under the EU Privacy Directive that address the collection of consent for cookies and similar technologies. The Alliance would also welcome guidance in the Regulations as to examples of acceptable just-in-time notices for collecting such consent.

IX. Topic 9: Additional Comments The Regulations Should Give the Agency Flexibility in Enforcement with Respect to Employee and B2B Data.

The CPRA is intended to be a consumer privacy law, and that is what California voters acted on. Moreover, other states have consistently exempted information derived from or related to employees and business representatives from the scope of their consumer privacy laws, largely because that type of information is already rather heavily regulated. As such, the Alliance respectfully recommends that the Regulations allow the Agency to refrain from taking enforcement action for alleged violations involving employee information or information of business representatives. The Agency should not waste valuable time and limited resources on pursuing violations that distract from the Agency's priority of protecting consumer privacy.

X. Conclusion.

It has never been more clear that a vibrant and thriving free press cannot be taken for granted. To that end, the responsible use of digital advertising is critical to assuring that independent media do not cease to exist. Aligning digital data practices with consumer expectations can contribute to improving readers' trust in news at a time when it is under threat, and can help make the advertising market more competitive by decreasing the network effects caused by the consolidated and centralized data collection by third parties.

The Alliance looks forward to working with the Agency to craft forward-thinking Regulations that balance consumer privacy with the needs of independent journalism (which is so critical to a functioning democracy), and that could serve as a model for other states and jurisdictions around the world.

Sincerely,

Danielle Coffey
EVP & General
Counsel
News Media Alliance

From: Info [info@informationaccountability.org]
Sent: 11/8/2021 3:54:25 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 ; Comments by the Information Accountability Foundation in response to the CPPA CPR
Attachments: IAF Comments in Response to the California Privacy Protection Agency CPR_11.08.2021.pdf

Hello,
Please see the attached comments by the Information Accountability Foundation (IAF) in response to the California Privacy Protection Agency CPR. The IAF is a non-profit research and education think tank, whose mission is collaborative scholarship and education on the policies and processes necessary to use data responsibly in an observational age, while enabling a trusted digital ecosystem that serves people.

Comments by the Information Accountability Foundation in response to the California Privacy Protection Agency (CPPA) CPR.

November 8, 2021

The Information Accountability Foundation (IAF), thanks the California Privacy Protection Agency for the opportunity to provide comments developing new regulations and potential changes to existing regulations.

The IAF is a non-profit research and education think tank, whose mission is collaborative scholarship and education on the policies and processes necessary to use data responsibly in an observational age, while enabling a trusted digital ecosystem that serves people. IAF scholarship is based on three core beliefs:

- To enable and achieve the benefits of a global digital ecosystem, organizations must be able to think with data and responsibly engage in knowledge creation (thinking with data).
- To be trusted, organizations must be accountable, responsible, and answerable and be prepared to demonstrate their accountability.
- To enable beneficial, data-driven innovation while protecting individuals and society from the potential harms that may arise from data processing in the digital age, frameworks must be based on risk assessments and effective and risk appropriate data governance.

These views reflect the views of IAF staff and do not necessarily reflect the views of the IAF board of trustees, contributors, or broader community. We will be commenting specifically on items 1, and 8.

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

As the interests of multiple stakeholders increase and the expectation that organizations be accountable and be prepared to demonstrate that processing is trustworthy, risk assessments about data pertaining to people are a critical and necessary lynchpin of operational processes for evaluating the risk to consumers' privacy and security.

Security, particularly as it pertains to data, is a well-defined concept, with those definition well understood. For example, the Graham, Leach, Bliley Act Safeguards Rule has been a model for data security for a generation. Privacy, on the other hand, does not have a consensus definition. Instead, it is a concept best defined by its three elements:

- Respect for a space from observation;
- An interest in controlling the data that defines one's personhood;
- The right to fair outcomes when data pertaining to individuals is processed.

Trustworthy processing is the cornerstone of the digital and data-driven economy. Trustworthy processing is the foundation necessary to maintain California's leadership as the largest economy in the U.S. and as the 5th largest economy in the world. All three elements come into play when assuring trustworthy processing.

The power and potential of digital technologies and data for California citizens, society, and organizations depend on their effective use of the digital technology ecosystem by allowing data to be processed responsibly. One way to enable more sophisticated usage is to enhance trust in the digital environment. One way to do that is to empower consumers and organizations to better manage digital risk. Data used in a thoughtful, responsible, transparent manner will enhance trust in digital processes. For this reason, the risk of organizations not using data to create value, reticence risk, is just as big a risk as organizations misusing data. The risk of not using data to achieve legitimate ends is directly related to privacy's third element, fair outcomes. To achieve trustworthy processing, it is critical to mitigate, as much as possible, the detriments to all three elements. Data subject rights speak directly to the first two elements. However, in the end the responsible company must have a program for identifying and mitigating the privacy and security risks, including the use of PIAs and security threat risk assessments.

Since 2014, the IAF has led multistakeholder research projects that describe ethics-based assessment frameworks for complex and potentially risky processing. This is particularly targeted to fair outcomes. The Assessment Framework functions as a governance model, and should be used processing reach key milestones or decision points. This will vary from sector to sector, industry to industry, and organization to organization.

Concept- Organizations should determine the reasons for using all the intended data sets, new data created, chances for new insights, usefulness of those insights and possibilities of further application. The results of this process should be presented to decision makers for a determination about whether to proceed to the actual Discovery phase, also known as knowledge creation (we describe knowledge creation in more depth in our response to question 8).

Discovery- Generating new insights through processing takes place during the Discovery phase. It's during this phase that data is aggregated, formatted, enhanced or created.

Application- Between completing of the Discovery phase and the beginning the Application phase, a decision to move forward or not should be made. This is the time when the organization must determine whether the processing will create real benefits and who will receive those benefits; whether the insights will be sustainable once analytics begins; and whether the application is respectful and fair to individuals.

This two-phased approach to knowledge discovery and knowledge application was first described in a paper co-authored by the IAF's chief strategist Martin Abrams, "Big Data and Analytics: Seeking a Foundation for Effective Privacy Guidance."

Review- Ongoing reviews are required to validate that the implemented controls for processing are working. An ethical review should take place when routine reviews of new applications of data are scheduled. The level of the ethical review should be proportional to the evolution of the processing programs. New data sets may have been introduced, or processing shortcuts may have been developed. If changes are extensive, the ethical review should be similarly robust. A trustworthy organization is the one that makes prudent decisions that get the balance right. For example, individuals have an interest in a space free from observation and controlling their data, but they also have an interest in quality health outcomes and a healthier society.

The IAF encourages the CPPA to promote and support the use of Accountability-based risk assessment frameworks by organizations.

1.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."

This is the most straightforward consideration, as there are widely-recognized, standards-based cybersecurity audits that are recognized nationally and beyond, which many companies already apply today: SOC 1,2 and 3, the ISO 270xx series, and the U.S.-developed NIST framework. These cybersecurity assessments are usually completed by external 3rd party experts, and can also include privacy risk components, and can be blended with the ethics-based processing risk assessment described in section 1.c. The CIS Critical Security Controls (v8) also would meet this requirement when the assessment is conducted by an external expert. The CPPA should actively advocate for and support organizations' use of the above-described cybersecurity frameworks when assessed by external experts.

1.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.

A risk assessment should include the following elements (a sample template is at the end of this document). The organization should describe the processing project **Characteristics**, whether the processing is **Beneficial** to individuals, and is the processing **Fair**.

Describe the project Characteristics
Purpose: Understand the purpose and intended outcomes of the project.
Sources: Understand the sources of data to be used in the project.
Preparation: Understand the pre-processing that will be done before the analysis.
Contractual and legal conditions: All processing and applications should be within the context of the conditions associated with the data.

Accuracy: Evaluate the accuracy of the consolidated data.
Insights: Understand what insights are expected from the analysis.
Outcomes: Check to see that the insights and actions are progress from legacy processes.
Accountability: Identify the individuals who are responsible for the project.
Stakeholders: Identify all the stakeholders and their concerns.

Determine the Beneficial aspects of the project
Benefits: What are the benefits for each stakeholder identified above that are expected to come from the analysis?
Risks/Mitigations: What are the risks to each stakeholder? How are the risks mitigated?

Is the project Fair
Fairness: Could the result be considered unfair to individuals and if so, how.
Balancing: Evaluate whether the residual risks and benefits balance individual and societal interests.

1.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.

A privacy regulator typically has a mandate to protect individuals in almost all their roles, market-based and non-market harms. It is important to recognize that it is more often than not the context in which data are used that creates real risks of inappropriate consequences to individuals. In many ways, this concept is already recognized in United States law. For example, under the Fair Credit Reporting Act, the risk of consequences when using consumer reports for employment decisions is different than when using the same report for credit purposes. Therefore, different protections are built into the employment report process. Other examples which require careful scrutiny and possible prohibition are those described in the NIST Privacy Framework Roadmap, along with a carefully articulated "cross-walk" which describes how the NIST Privacy Framework aligns with CCPA and CPRA.

8. Definitions and Categories.

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

Many beneficial advances in "knowledge creation" and scientific research come from combining data from multiple sources both internal to the organization and from external sources. Knowledge creation is the generation of insights about people that originates with data that pertains to people in general and not a specific individual or set of individuals (and is distinctly separate activity from "knowledge application").

The process of "knowledge creation" has been called "thinking with data," and the process of "knowledge application" has been called "acting with data." Understanding the difference between knowledge creation and knowledge discovery and the purposes for which they are being undertaken is critical to understanding how they should be regulated

Knowledge creation, which is the pathway to the future, is conducted for two different research purposes: (1) scientific, and (2) commercial. Knowledge creation when used as part of advanced data analytics is the engine that drives the digital economy in a society.

Like knowledge creation for scientific purposes, knowledge creation for commercial purposes requires its own set of controls. To begin, an organization must: have a legitimate objective to conduct knowledge creation, conduct and document a risk assessment, and establish an internal oversight mechanism.

Treating knowledge creation and knowledge application the same has the unintended consequence of overburdening the organizations that are the engines for digital innovation (e.g., innovators in medical devices, transportation, education, design, and services.) There is a great deal of concern about surveillance market players, but they are not the only knowledge creation innovators.

The Information Accountability Foundation (IAF) has advocated for many years that there should be a distinction between knowledge creation (thinking with knowledge) and knowledge application (acting with knowledge).

Thank you for the opportunity to respond to the consultation. Barbara Lawler was the lead author of these comments. If you have follow-up questions you may reach her at blawler@informationaccountability.org. These comments are followed by some supplemental content.

Supplement to response 1.c.
Sample Risk Assessment worksheet that includes ethical considerations and fairness to the full range of stakeholders.

Contextual Assessment Worksheet

The purpose of assessment is to identify the issues that must be resolved to assure an organisation's big data project is fair to the full range of stakeholders (please see Part A, Unified Ethical Frame). The questions below have been designed to illuminate those issues for decision makers and create a record for review. (Version 1.5)

Questions	Explanatory Commentary	Answers
CHARACTERISING THE PROJECT		
Purpose: Understand the purpose and intended outcomes of the project. Provide a project overview that describes the main purpose of the project. Is the primary purpose of the project to generate new insights or to expand on insights from a previous project or previous work?	Consider such purposes as: ▪ Marketing or risk management ▪ Building/enhancing solution and product capability ▪ Distribution network ▪ Enhancing brand experience ▪ Marketing: traditional direct mail, email, telemarketing, digital advertising, etc. (Note: Data flow mapping may be a technique that can help answer these questions.)	
Sources: Understand the sources of data to be used in the project. What are all the sources of the data?	Data Origins: ▪ Provided by the individual ▪ Scraped from the web ▪ Observed in some other fashion ▪ Derived from other data	

Is the source data from trusted sources? What actual data elements are found in the data? How frequently should the source data be updated/refreshed? How was the data from each source originated? Can the source data be kept current over time? If not, is there an adequate replacement? Are there legal, policy, contractual, industry, or other obligations linked to the data? Is the data linkable to a particular individual or not? Is the source data structured or unstructured or both?	▪ Inferred from analytics Linkability: ▪ Personally Identifiable Information/personal data ▪ Pseudononymous ▪ Device Identifiable Information ▪ De-Identified ▪ Aggregate Industry obligations include codes of conduct.	
<u>Preparation:</u> Understand the pre-processing that will be done before the analysis. What work will be done to put the data in a consistent format? How will errors and redundancy in the data be identified and dealt with? How will the data sources be consolidated for analysis?	Steps in Preparation: ▪ Data standardisation ▪ Data hygiene, integrity and accuracy ▪ Data source validity ▪ Data integration (consolidation)	

Will further synthesising of the data be necessary?		
<u>Contractual and legal conditions:</u> All processing and applications should be within the context of the conditions associated with the data. Has there been a review of all obligations associated with the data? Is the data being used within the context of its origination? If the data is originated by others, are conditions on the data being respected? If the project moves forward, will the project security be adequate/proportional to the risks related to the data? Would the application of insights be seen as ethical and respectful if publicly exposed?	Obligations associated with the data include: ▪ Laws ▪ Regulations ▪ Policies ▪ Contracts ▪ Industry codes	
<u>Accuracy:</u> Evaluate the accuracy of the consolidated data. What is the accuracy of the consolidated data set to be analysed? Are there concerns about the quality of the final data set to be analysed?		

<u>Insights:</u> Understand what insights are expected from the analysis. What is the output from the analysis? What will the insights from the analysis be used for? Who will use the resulting insights? How long might an insight endure? What is the half-life of the insight? For how long are the insights repeatable? Can the application of the insights impact behaviour in a manner that could reduce the predictive value of the insights over time? Will evolving trends impact public expectations or public policy in a manner that will impact long-term durability?	(NOTE: A demo can be useful in helping to understand the insights.)	
<u>Outcomes:</u> Check to see that the insights and actions are progress from legacy processes. Will the project result in better outcomes than currently available? Which stakeholders have positive outcomes? Negative outcomes? Neutral outcomes? Can the same or similar outcomes be achieved with fewer risks (e.g., possibly done with less robust data)?		

Accountability: Identify the individuals who are responsible for the project. Who has ultimate project ownership? Who is accountable for the various phases of the project? Do the insights contemplated by the project seem inappropriate, creepy, intrusive or rude?	Project team includes: ▪ Data capture/acquisition ▪ Data preparation/management ▪ Oversight for restrictions (legal or contractual) ▪ Appropriate application of the analysis/insights	
Stakeholders: Identify all the stakeholders and their concerns. Who are all the stakeholders related to both the analysis and the use of the resulting insights? What stakeholder concerns may arise? Are there other factors that should be taken into account?	Possible stakeholders include: ▪ Individuals ▪ Organisations (including businesses and non-governmental organisations) ▪ Political entities/government ▪ Society/public-at-large/community ▪ Others Other factors include: ▪ Cultural differences ▪ Commonly held societal values ▪ Compatibility with organizational values ▪ Compatibility with social norms regarding the use of sensitive information	

BENEFICIAL		
Benefits: What are the benefits for each stakeholder identified above that are expected to come from the analysis?	There may be more than one benefit for a stakeholder. Obvious benefits can include: ▪ Personalization ▪ Health ▪ Education	

	▪ Economic opportunity ▪ Other (please specify) ▪ Society as whole	
Risks/Mitigations: What are the risks to each stakeholder? How are the risks mitigated?	Risks to stakeholders take into account: potential impacts of false positives or negatives.	
Risk/Benefit Analysis: Are the mitigated risks sufficiently balanced by the benefits? What are the residual risks after mitigation?	The risk/benefit analysis should be documented.	
FAIR		
Could the result be considered unfair to individuals? If so, how? Are there Issues that could arise from this project? Will the residual risks and benefits balance individual and societal interests? From your perspective as the project owner, are you confident that the interests of stakeholders are balanced in a fair fashion?	Issues include: ▪ Regulatory and enforcement ▪ Media ▪ Public backlash ▪ Breaking Contracts ▪ Employee backlash ▪ Discriminatory affects such as economic opportunity, physical security, physical wellbeing and limiting self-determination.	

From: Annalee Akin [redacted]
Sent: 11/8/2021 4:11:34 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 CPRA Comments - California Advocates - Mike Belote
Attachments: CPPA - CPRA Comments. 11.8.21.pdf

[EXTERNAL]: [redacted]

Good afternoon,

Please find comments from Mike Belote of California Advocates, Inc. attached here in connection with the California Privacy Protection Agency Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020.

Please let me know if there is any additional information needed.

Thank you,
Annalee

Annalee Akin
Legislative Assistant
California Advocates, Inc.
1112 11th Street
Sacramento, CA 95814
[redacted]

CALIFORNIA ADVOCATES, INC.

Michael D. Belote
Dennis K. Albiani
Faith Lane Borges
Cliff Costa
Anthony Molina

November 8, 2021

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

RE: Comments in connection with the California Privacy Protection Agency Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020

Dear California Privacy Protection Agency:

We have discussed the forthcoming California Privacy Rights Act (CPRA) regulations with various clients represented by our firm and appreciate the opportunity to provide input. The California Privacy Protection Agency's (CPPA's) work to enact the CPRA reflects an important commitment to protecting Californians' constitutionally protected right to privacy. Our clients believe that it is possible to both respect user privacy and provide innovative, data-driven services at the same time. Striking this balance is crucial--we and our clients want users of all products and services to be confident that their data is being processed in a transparent and respectful way and to keep developing and deploying privacy preserving architectures and technologies to help achieve this.

We appreciate the CPPA's proactive efforts to shape positive regulation and respectfully offer the following comments on certain key issues where the CPPA has the power to adopt rules that could clarify ambiguities in the CPRA, mitigate the risk of unintended negative consequences, and improve the overall effectiveness of the law in protecting consumer privacy. As discussed in more detail below, we encourage the CPPA to support and encourage privacy-preserving technologies and design choices including, for example, by: (1) confirming that information linked to a random, non-static, rotating, or resettable device-generated identifier may fall outside the definition of "personal information"; and (2) designing regulations that align with robust privacy laws and regulations in other jurisdictions around the world.

I. The CPPA should support and incentivize the use of privacy-preserving technologies and design choices, including by providing guidance around sample technologies that fall outside of the definition of "personal information" in the CPRA.

A. Privacy-preserving technologies play an important role in safeguarding consumer privacy.

Our clients use innovative privacy technologies and techniques ("privacy-preserving technologies" or "PPTs")[1] designed to minimize how much of an individual's personal information they — or anyone else — can access. PPTs protect the privacy of personal or sensitive information and provide critical protections for consumers. For example, they reduce or minimize the amount of data that businesses hold about individuals and empower individuals to retain control of information about themselves. These rapidly evolving technologies also support innovation and data sharing while reducing the risks of identity disclosure, either by businesses or a potential bad actor in the event of a breach, and help prevent information (*e.g.*, related to identity or location) from being associated with individuals.

PPTs can also significantly benefit consumers by, for example, ensuring that their consent preferences remain up to date and apply across data sets, minimizing the amount of data that is collected and shared, providing transparency about their transactions and activity online, enhancing the security of data processing, verifying or anonymizing users and user credentials, and allowing consumers to exercise more control over which pieces of personal information are shared with and used by third parties.

We encourage the CPPA to support and incentivize the use of PPTs as effective tools with which to protect consumers' personal information.

B. The CPPA should support consumer privacy and the use of PPTs by confirming that "personal information" excludes data identified by random, non-static, rotating, or resettable identifiers.

This rulemaking process provides the CPPA with an opportunity to greatly enhance consumer privacy and the underlying goals of the CPRA, including by confirming that the term "personal information" excludes data identified by non-personally identifiable identifiers such as those that are random, non-static, rotating, or resettable.

---

[1] *See, e.g.*, Privacy Enhancing Technologies – A Review of Tools and Techniques, a report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada (Nov. 2017), https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711; Privacy enhancing technologies for trustworthy use of data, UK Information Commissioner's Office Centre for Data Ethics and Innovation Blog (2021), https://cdei.blog.gov.uk/2021/02/09/privacy-enhancing-technologies-for-trustworthy-use-of-data/.

Under the CPRA, the definition of "personal information" includes information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[2]

If the term "personal information" were interpreted overly broadly so as to include data identified solely by a random, non-static, rotating, or resettable device-generated identifier, for example, a business that maintained such data may be forced to build a way to link the information to identified consumers solely to respond to consumers' CPRA rights requests. Doing so would be contrary to data minimization principles, as it would effectively force companies to collect personal information when they otherwise would not need to do so, and to send it back to their servers rather than keeping it on the user's own device. It would also undermine the privacy interests of consumers (including those who may not exercise their specific CPRA rights) that seek out PPTs *because* they do not require the collection of personally identifiable information.

Linking identified consumers to data that was previously keyed only to random, non-static, rotating, or resettable device-generated identifiers also increases the risk that private information about the individual could be revealed in the event the data is subject to unauthorized access (such as a data breach). A key benefit of the use of non-personally identifiable identifiers is that neither the business that collects the data, nor any unauthorized recipients of the data (such as a hacker) learns about particular identified consumers. Keeping such information on the user's device, rather than transmitting back to company servers, further protects the individual's privacy.

An overbroad interpretation of personal information also would unnecessarily burden businesses that currently incorporate PPTs and eliminate incentives to use PPTs in future products and services, if they will ultimately be forced to link those non-personally identifiable identifiers to identified consumers, anyway. The result would clearly lead to bad results for consumers: businesses would end up collecting more personally identifiable information than needed and transmitting more of it back to their servers, solely because of CPRA compliance obligations.

It is important that the CPPA provide clear guidance on this point sooner rather than later. For example, it takes time and resources to develop and implement PPTs, such as the use of random, non-static, rotating, or resettable device-generated identifiers. These technologies,

[2] Assembly Bill No. 694 § 3, amending § 1798.140.

while important to advancing individual privacy, often have many moving parts[3] and take years to develop and test. In addition, many smaller companies, and startups in particular, will need a reasonable degree of certainty that these technologies will be supported by the law to justify the additional work and investment that is needed to develop and implement them for use after the CPRA takes effect. Knowing that the CPPA supports their use, in part by allowing for flexibility in how it interprets certain terms in the CPRA, will encourage even more development in this area.

C. *Supporting PPTs would align the CPRA with other key global privacy frameworks, such as the EU General Data Protection Regulation (GDPR).*

We appreciate the protections set forth in the CPRA and believe that reasonable harmonization with other key privacy frameworks will help to achieve the CPRA's goals of strengthening consumer privacy while enabling innovation.

For example, the GDPR recognizes[4] that it is not always possible to be certain when information relates to an "identifiable" individual, and it instead imposes an obligation on companies to conduct an assessment of the means reasonably likely to be used to directly or indirectly identify individuals. The GDPR further defines "personal data" to include information that relates to an "identified or identifiable natural person" and would therefore exclude data that is identified solely by a non-personally identifiable identifier.

We encourage the CPPA to craft regulations that align with this proven, workable approach. Such assessments have been part of the public discussion for years[5] and provide valuable guidelines on how to think about identifiable data in the context of providing enhanced privacy protections for everyone.

We support a pragmatic approach to defining identifiable information. We encourage the use of a framework that strikes a balance between protecting personal information and putting it to work for the individuals who want or need certain services. For example, we encourage the CPPA to consider what is necessary to achieve effective anonymization in detail and to recognize that the set of technical and organizational measures applied is a key factor to assess how to regulate certain information.

---

[3] *See, e.g.*, the U.S. Census Bureau's description of its years-long process to implement differential privacy to maintain the confidentiality of individuals' and households' data: https://www.ncsl.org/research/redistricting/differential-privacy-for-census-data-explained.aspx.

[4] *See* GDPR, Recital 26.

[5] *See, e.g.*, the Article 29 Working Party's paper on anonymisation techniques, focusing on "singling out," "linkability," and "inference" as the three key elements in assessing identifiability: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

II. We encourage a thoughtful, impact-based approach to the rules around automated decisionmaking and profiling.

We support the CPPA's work to provide individuals with increased control over automated decisions that are made about them. In an effort to have the most impact for consumers and avoid imposing unnecessary compliance costs on small businesses and other companies, we encourage the CPPA to prioritize guardrails for automated decisionmaking activities and technologies that may result in a high risk of harm to individuals.

There are countless automated decisions that occur every day that, while providing benefits to consumers in the form of easy-to-use products and services, do not present a significant risk of harm to consumers. For example, an online store may use automated decisionmaking technology to recommend products that may align with a consumer's interests. For many of these everyday automated decisions, if they were able to be altered on a case-by-case basis, it would significantly hinder the products and services that companies could offer.

Many of these lower-risk decisions are made on the basis of limited data collection, aggregated data, and data with short retention periods, reducing the potential for systemic tracking or monitoring. For example, a business offering a music streaming service may design features in order to make recommendations more personal and engaging by using automated decisionmaking. While the risks of these decisions are low, they provide benefits to consumers by cutting down on the time it takes to find the music they're looking for. They also benefit emerging artists who are keen for users to discover their music.

Overly broad concepts of automated decisionmaking could be interpreted to apply to almost every use of data. Such an interpretation would create significant compliance costs for small businesses and other organizations, including for example to adopt and implement novel processes for decisions, recommendations, and predictions. Moreover, applying strict rules to automated decisionmaking in lower-risk contexts, in particular, may deter businesses from using innovative technologies and deny consumers the benefit of valuable products and services that they rely on today.

There are some automated decisions that warrant additional protections, including decisions that impact the legal rights of or have a significant impact on a consumer. Both Colorado and Virginia have recently codified definitions of "decisions that produce legal or similarly significant effects concerning a consumer." Under Colorado law, for example, this term 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."[6]

To avoid stunting the development of innovative technologies, we encourage the CPPA to take a thoughtful, impact-based approach to automated decisionmaking regulations. Any regulations should consider when consumers may be able to opt out of automated decisions, including the standard for when an outcome could have a significant impact[7] on their lives. Such an approach would also align the CPRA with other strong privacy laws, such as the GDPR, thereby making it easier for companies to provide strong and consistent automated decisionmaking safeguards for consumers across multiple jurisdictions.

III. To encourage compliance efforts further, the CPPA should establish reasonable parameters for risk assessments.

While conducting risk assessments may be a new process for some businesses, many already are subject to existing global privacy frameworks that have long required risk assessments for processing that presents a potentially significant risk to consumers.

For example businesses that are subject to the GDPR already are required to undertake data protection impact assessments (DPIAs) for products and services that process personal information and many businesses have integrated these DPIAs into their product development efforts. Reviews required by the GDPR are comprehensive in nature, taking into account the data elements being processed, the purposes for which they are processed, whether the data is necessary for and proportionate to those purposes, and the existence of compensating controls to mitigate against any privacy risks. These assessments also include analyses of whether there is decision making relying upon algorithmic systems and the impact that such decision making has on individuals and their rights. Risk levels are assigned to all data uses, with re-review anytime there is a material change to the processing for which the assessment was conducted.

Permitting organizations to leverage existing assessments, such as DPIAs, will promote efficiency and reduce duplicative efforts by allowing businesses to use risk assessments across multiple jurisdictions. A standardized approach to these assessments will encourage further compliance by businesses, especially for smaller organizations with limited resources, providing increased protections for consumers. We encourage the CPPA to incorporate elements from

---

[6] Colorado Privacy Act, S.B. 21-190 (to be codified C.R.S. § 6-1-1303(10)).

[7] Other states, such as Virginia and Colorado, have adopted definitions of "decisions that produce legal or similarly significant effects concerning a consumer" in the context of the right to opt out of such decisions. These definitions generally recognize that opt-outs should be available for automated decisions in higher-risk areas, such as financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services.

these jurisdictions when crafting a framework for CPRA risk assessments. For example, the Irish Data Protection Commission's "Guide to Data Protection Impact Assessments (DPIAs)"[8] provides a helpful framework for organizations to consider when processing is likely to result in a high risk to consumers. And several supervisory authorities,[9] including the UK ICO, have drafted a helpful list of factors for organizations to consider when considering whether a risk assessment is prudent.[10] Following these global models for assessments would help ensure that California consumers enjoy the same high level of privacy protections that individuals in other jurisdictions enjoy.

Allowing businesses to leverage existing assessments also aligns with the approach taken by the Virginia legislature. Under the recently enacted Virginia privacy law, businesses are also required to conduct data protection assessments before engaging in certain types of personal information processing activities. The law provides that data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations will satisfy the controller's obligations under Virginia law if the assessments have a reasonably comparable scope and effect.[11]

Harmonizing the CPRA's approach with existing global frameworks will help businesses provide a strong, unified approach to protecting privacy and help ensure that Californians benefit from the highest levels of information privacy. A focus on consistent factors for assessing processing activities will set expectations for the industry and encourage companies to adopt a uniform approach, rather than focusing resources only on jurisdictions that set a higher standard.

IV. Conclusion

We support the CPPA's efforts to seek broad comment on how best to frame implementing regulations for the CPRA and look forward to opportunities to provide additional input as the

---

[8] https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20(DPIAs)_Oct19.pdf.

[9] *See* European Data Protection Board Opinions on the draft lists released by Member State supervisory authorities identifying data processing activities likely to result in a high risk and therefore require DPIAs, available at https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en?f%5B0%5D=opinions_publication_type%3A61&f%5B1%5D=opinions_topics%3A138.

[9] *See* European Data Protection Board Opinions on the draft lists released by Member State supervisory authorities identifying data processing activities likely to result in a high risk and therefore require DPIAs, available at https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en?f%5B0%5D=opinions_publication_type%3A61&f%5B1%5D=opinions_topics%3A138.

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when1.

[11] Virginia Consumer Data Privacy Act, S.B. 1392 (to be codified Va. Code Ann. § 59.1-576(D)).

rulemaking process continues. We encourage the CPPA to consider the foregoing points in its efforts to help ensure that the goals of the CPRA are met in a way that protects individuals and encourages privacy-protective innovations. Doing so will help harness the benefits that individuals can derive from transparent and respectful use of their data, provide further clarity to the CPRA's requirements, mitigate the risk of unintended negative consequences, and improve the overall effectiveness of the law in protecting consumer privacy.

***

We thank the CPPA for considering these comments in its rulemaking process.

Sincerely,

Michael D. Belote
President, California Advocates, Inc.

From: Ferrell, Peter [redacted]
Sent: 11/8/2021 4:27:23 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 - NEMA Comments
Attachments: NEMA Comments - No. 01-21.pdf

[EXTERNAL]: [redacted]

Ms. Castanon,

On behalf of the National Electrical Manufacturers Association, please find our comments regarding proceeding number 01-21.

Should you need additional information, please do not hesitate to contact me.

Sincerely,
Peter Ferrell
Manager, Connectivity and Data Policy
National Electrical Manufacturers Association
1300 17th Street North, Suite 900
Arlington, VA 22209-3801
[redacted]

National Electrical Manufacturers Association

The association of electrical equipment and medical imaging manufacturers
www.nema.org

November 8, 2021

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

RE: Response to Invitation for Preliminary Comments on Proposed Rulemaking (Proceeding No. 01-21)

The National Electrical Manufacturers Association ("NEMA") is the leading trade association representing manufacturers of electrical and medical imaging equipment. The purpose of this letter is to introduce the electroindustry to the California Privacy Protection Agency ("Agency") as it invites public input and preliminary comments on proposed rulemaking under the California Privacy Rights Act ("CPRA") of 2020.

NEMA represents approximately 325 companies that manufacture safe, reliable, and efficient products and systems across 54 product sectors. Our combined industries account for more than 370,000 American jobs in more than 6,100 facilities covering every state. Additionally, the electroindustry produces $130 billion in electrical and medical imaging shipments annually, with $38 billion exported. In California specifically, 72 of our Member companies maintain 164 facilities, employing more than 24,000 people.

The products and systems NEMA Members produce are used and experienced by consumers daily in myriad ways, from smart lightbulbs in the home, to automated temperature control systems in connected buildings, to charging stations for clean electric vehicles. Many of these products are more effective in their application by the input of data received from consumers and their operating environments. Therefore, NEMA takes seriously the proper handling and processing of data and the security of that data from tangible and cyber threats.

The rich diversity of electroindustry products requires that NEMA Members invest significantly in developing and maintaining the integrity of supply chains rooted in privacy, security, and quality in order to bolster both public and private confidence in those products. Many products require the cybersecurity of operational technology ("OT") *in addition to* information technology ("IT"). This means that the Agency should not attempt to implement a single, "one-size-fits-all" approach to securing consumer data and control systems.

In making OT products secure, NEMA Members have collaborated with national and international Standards development organizations to create trusted and certifiable cybersecurity Standards, including:

- **National Institute of Standards and Technology ("NIST") Cybersecurity Framework** (https://www.nist.gov/cyberframework). The Framework is a widely used and respected set of guidelines and best practices businesses use to mitigate cybersecurity risks. The Framework allows a company to tailor and scale their cybersecurity posture based on their needs and resources. The Framework also incorporates elements from other cybersecurity Standards, including the two immediately listed below.

- **International Society of Automation ("ISA")/International Electrotechnical Commission ("IEC") 62443 Series of Standards** (https://www.isa.org/isa99/). These standards and technical reports relate to securing Industrial Automation and Control Systems ("IACS") by providing a

systemic and practical approach to cybersecurity for industrial control systems. They also provide a flexible framework to address and mitigate security vulnerabilities in IACSs. Every stage and aspect of cybersecurity is covered, from risk assessment through operations.

- **International Organization for Standardization ("ISO")/IEC 27001 Family of Standards** (https://www.iso.org/isoiec-27001-information-security.html). Also known as the ISO 27000 series, these Standards are a collection of best practices to help businesses improve their information security by specifying requirements in their information security management systems.

Additionally, NEMA itself has published the Cyber Secure Supply Chain ("CPSP") Series of Standards, viable best practice documents which many electrical and medical imaging manufacturers implement to secure in their supply chains, operations, and products from cyber threats. They include:

- **NEMA CPSP 1-2015**: **Supply Chain Best Practices** (https://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx). This document identifies a recommended set of supply chain best practices and guidelines that electrical equipment and medical imaging manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation.

- **NEMA CPSP 2-2018**: **Cyber Hygiene Best Practices** (https://www.nema.org/Standards/Pages/Cyber-Hygiene-Best-Practices.aspx). This document identifies a set of industry best practices and guidelines for electrical equipment and medical imaging manufacturers to help raise their level of cybersecurity sophistication in their manufacturing facilities and engineering processes.

- **NEMA CPSP 3-2019**: **Cyber Hygiene Best Practices-Part 2** (https://www.nema.org/Standards/Pages/Cyber-Hygiene-Best-Practices-Part-2.aspx). This document identifies industry best practices and guidelines that electrical equipment and medical imaging manufacturers may consider when providing cybersecurity information to their customers. These practices and guidelines are meant to help customers effectively manage their cybersecurity expectations as they use the equipment within the context of their respective markets (e.g., commercial and residential buildings, industrial equipment, the electrical grid, hospitals, and surface transportation). The document also provides suggestions for how customers can work with their respective manufacturers to improve the customer's level of cybersecurity through industry best practices and guidelines.

The adoption of industry-developed, internationally recognized, and technology neutral cybersecurity Standards for IT and OT systems will be a critical component to ensuring the proper handling and processing of sensitive personal information by the electroindustry. The Agency should review these Standards, along with others, and incorporate them as appropriate into future proposal developments.

In its invitation, the Agency asks for input on the following topics:

> *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."*

Meaningful audits are rested in conformity assessments, where standardized requirements can be weighed against objective evidence and attested to by an independent party. As noted above, cybersecurity postures vary by technology application; therefore, cybersecurity audits should be performed using recognized Standards designed to validate a given posture. Electroindustry businesses

should be permitted to apply existing Standards and certifications, including conformity with the **NIST Cybersecurity Framework**, **ISA/IEC 62443**, **ISO/IEC 27001**, and the **NEMA CPSP** in meeting any Agency audit requirements.

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

The Agency should define what a "significant risk" entails which might initiate a cybersecurity audit. Furthermore, the definition should be tailored to conform with the cybersecurity posture a business would be audited against.

> *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.*

After a company has submitted a risk assessment, additional assessments should not be required unless there has been a change in the Standards a company uses to be secure. This ensures that the Agency has the most current and accurate information for an evaluation. Furthermore, any risk assessment should align with the definition of "significant risk" referenced above.

NEMA counts on the Agency's careful consideration of these comments on behalf of the electroindustry. Agency decision-making will benefit from continuing its outreach to the regulated community, and NEMA plans to particulate fully in future proceedings on this important topic. If you have any questions or need more information, please contact Peter Ferrell, Manager, Connectivity and Data Policy, at 202-841-3200 or peter.ferrell@nema.org.

Sincerely,

Philip A. Squair
Vice President, Government Relations

From: Mariam Abdel-Malek [redacted]
Sent: 11/8/2021 4:48:26 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: Preliminary Comment on Behalf of Pinterest - PRO 01-21
Attachments: Pinterest CPRA Preliminary Comment .pdf

[EXTERNAL]: [redacted]

To Whom It May Concern,

Attached, please find Pinterest's comments with respect to the California Privacy Rights Act ("CPRA"). We thank the Agency and staff for considering these comments and for its efforts to provide businesses clarity with respect to compliance with the law.

Please do not hesitate to reach out with any additional questions.

Respectfully,

Mariam Abdel-Malek | Privacy Counsel | [redacted]

Preliminary Comment on Behalf of Pinterest

November 8, 2021

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

To Whom It May Concern:

Please find below Pinterest's comments with respect to the California Privacy Rights Act ("CPRA"). We thank the Agency and staff for considering these comments and for its efforts to provide businesses clarity with respect to compliance with the law.

Pinterest is a visual discovery engine where people around the world go to find visual recommendations on a wide variety of interests. Our mission is to bring everyone the inspiration to create a life they love, and it is our guiding light in how we have created Pinterest, developed our products, and shaped our policies. Automated decision-making is what makes delivering personalized recommendations possible. This technology ensures that Pinterest users who are interested in home renovation, gardening ideas, or new dinner recipes, can quickly and easily find what they're looking for. This core functionality is what users expect when they join Pinterest.

The Agency has requested comments concerning "consumers' access and opt-out rights with respect to businesses' use of automated decision-making technology" under Cal. Civ. Code, § 1798.185(a)(16).[1] On this topic, Pinterest urges the Agency to align its regulations concerning automated decision-making with those imposed by other omnibus consumer privacy laws.

Specifically, any rules governing automated decision-making should be limited to circumstances where such decision-making produces adverse legal or similarly serious effects. Such a standard would be consistent with the General Data Protection Regulation ("GDPR")—a law upon which the CPRA was modeled, and which imposes enhanced transparency and choice obligations only with respect to automated decision-making that "produces legal effects concerning" data subjects or that otherwise "similarly significantly affects" them.[2] Adopting such a standard would

[1] *See* Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020, *available at* https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

[2] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter "GDPR"] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1617842154965 (arts. 13(2)(f), 14(2)(g), and 15(1)(h), each requiring transparency but only for automated decisionmaking covered by art. 22(1), which gives an opt out right for automated decisionmaking/profiling when decisions produce legal or similarly significant effects).

also align with analogous laws that will take effect at the same time as the CPRA. For instance, Colorado and Virginia's consumer privacy laws regulate the analogous term of "profiling" only to the extent such profiling produces "legal or similarly significant effects concerning a consumer."[3] Limiting rights around automated decision-making in this way would provide consumers with an important protection against legally-recognized harms and provide flexibility to encompass future harms without chilling the development of valuable consumer services.

Any effort to regulate automated decision-making that does not result in adverse legal or similarly significant effects would be overly broad, would require companies to build inconsistent compliance solutions, and would provide no corresponding benefit to consumers. While consumers certainly should have the ability to understand, for instance, the logic behind any automated decision-making that results in them being denied credit, housing, employment, or insurance, requiring businesses to explain to consumers the logic used to highlight or feature some ordinary commercial content over other such content would not serve any meaningful policy goal.

The Agency should, furthermore, make clear that automated decision-making concerns only decision-making accomplished entirely via automation and not the result of any human intervention, consistent with the plain meaning of the term and the GDPR.[4]

Finally, the Agency should be cognizant that its rulemaking authority with respect to automated decision-making concerns only opt outs and transparency obligations provided under the law and does not empower the Agency to, for instance, impose on businesses an obligation to allow consumers to opt out other than from the sale or sharing of their personal information and certain uses of their sensitive information.

Respectfully submitted,

Mariam Abdel-Malek
Privacy Counsel

---

[3] *See* Colo. Rev. Stat. § 6-1-306(1)(a)(C); VA. Code Ann. § 59.1-573(A).

[4] GDPR, art. 4(4) (profiling refers to "any form of *automated* processing") (emphasis added); GDPR, art. 22(1) (opt out right does not apply when decisions are "based *solely* on automated processing") (emphasis added).

From: Lisa Quaranta [redacted]
Sent: 11/8/2021 3:51:22 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: California Credit Union League Comment Letter re PRO 01-21
Attachments: CNCUL-CommentLetter-CPRA-Request for Comments - SIGNED 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.

Hello.

Attached please find the California Credit Union League's comment letter re: PRO 01-21 – preliminary comments on proposed rulemaking under the California Privacy Rights Act.

We appreciate the opportunity to comment on this matter and for considering our views.

Thank you,

Lisa Quaranta
Vice President, Regulatory Advocacy & Compliance
[redacted] | [redacted]
[redacted] | www.ccul.org

California NEVADA

California
CREDIT UNION LEAGUE

November 8, 2021

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

Via Email (regulations@cppa.ca.gov)

Re: Comment on Invitation for Comments Regarding California Privacy Rights Act of 2020 (PRO 01-21)

Dear Ms. Castanon:

I am writing on behalf of the California Credit Union League (League), one of the largest state trade associations for credit unions in the United States, representing the interests of approximately 230 California credit unions and their more than 11.6 million members.

On September 22, 2021, the California Privacy Protection Agency (CPPA) issued an invitation for comments as part of its preliminary rulemaking activities in connection with the administration and enforcement of the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA) (collectively, CCPA/CPRA).

The League has significant concerns regarding the CCPA/CPRA and respectfully offers the following comments.

I. Responses to Invitation for Preliminary Comments

A. Audits Performed by the Agency (Item 3)

Calif. Civil Code §1798.199.65 gives the CPPA the authority to audit businesses' compliance with the law. Absent clarification, credit unions may be subject to the CCPA/CPRA, and therefore to audits performed by the CPPA, and CPPA's enforcement authority could extend to both state and federally chartered credit unions.

As financial institutions, credit unions are already among one of the most highly regulated industries. California's state-chartered credit unions are licensed and regulated by the California Department of Financial Protection and Innovation (DFPI), and the National Credit Union Administration (NCUA) regulates federal credit unions as well as federally insured state credit unions. Additionally, credit unions are subject to federal Consumer Financial Protection Bureau (CFPB) oversight, among others. Credit unions currently undergo robust examinations by their regulatory agencies, which includes their compliance with applicable privacy and data security laws and regulations. We are concerned that potential audits conducted by CPPA would be unjustifiably intrusive, burdensome, and overreaching for credit unions. The burden of these additional audits on smaller financial institutions could be especially significant. Therefore, we believe that a clear exemption is warranted. However, if the CPPA is unwilling to provide such an exemption for credit unions, then it must provide guidance as to how credit unions can comply without unnecessarily burdening the credit union industry. At a minimum, coordination with state and federal primary regulators would be warranted.

B. Consumers' Right to Delete, Right to Correct, and Right to Know (Item 4)

The CPRA has amended the CCPA to add a new right: the Right to Request Correction of Inaccurate Personal Information (Calif. Civil Code §§1798.106 and 1798.130.

The following outlines our specific issues:

- *Definition of the Term "Inaccurate"*

The CPRA does not discuss what the term "inaccurate" means. We believe the lack of clarity in this area could potentially create confusion and possible unintended violations of CPRA. Therefore, we recommend the draft regulations define the term "inaccurate" in order to ensure that covered credit unions have a clear understanding of the accuracy and integrity of the information relating to consumers. Additionally, we are looking for assurances that good faith efforts to verify information and correct inaccurate information, and the refusal to make requested corrections due to fraud prevention concerns with not be penalized.

C. Definitions and Categories: Personal Information (Item 8(a))

Calif. Civil Code §1798.140(v)(1) identifies enumerated examples of "personal information" that *may be* deemed as identifiable, but *not always* identifiable personal information. We believe that further clarification is needed on whether certain of the exemplary examples of personal information are inherently identifiable to a consumer and therefore would constitute as "personal information."

D. Definitions and Categories: Sensitive Personal Information (Item 8(b))

Under Calif. Civil Code §1798.140(ae), "sensitive personal information" is defined to include, for example, "[s]ocial security numbers, information that allows access to a financial account, precise geolocation information, information about race, ethnicity, sexual orientation, religious or philosophical beliefs, contents a consumer's mail, email, and text messages, and genetic data."

We do believe that further clarification is needed regarding the term "sensitive personal information." For example, it would be meaningful if the CPPA were to clarify, among other things: (1) what constitutes "inferring characteristics;" (2) what types of information in "the contents of a consumer's mail, email and text messages" would be considered to be "sensitive personal information"; and (3) what the phrase "[p]ersonal information *collected and analyzed concerning a consumer's sex life or sexual orientation*" would mean in the context of "sensitive personal information." For example, does this last phrase include a simple request for marital status, which is commonly collected in connection with loan applications and other transactions that may be impacted by California's status as a community property state.

II. General Comments

A. The Credit Union Difference

The League supports the spirit of the law; however, it is important that the CPPA understand the credit union difference. Credit unions are member-owned, democratically governed, not-for-profit cooperatives whose purpose is to promote thrift and improve access to credit for their member-owners, particularly those

of modest means. As not-for-profit entities, credit union earnings are passed on to their member-owners in the forms of reduced fees, higher savings rates, and lower loan rates. Credit unions exist for the financial benefit of their member-owners, but they are ultimately driven by the philosophy of people-helping-people.

The credit union structure is vastly different than for-profit entities. "Owners" are not proprietors or shareholders in a business whose only goal is that the business maximize profits. Instead, they are members of a not-for-profit cooperative with a volunteer board of directors democratically elected by and from among its members. Consumer personal information collected by credit unions is the personal information of its member-owner consumers in order to provide them with the products and services they desire.

Credit unions are the original consumer financial protection advocates. In addition, as highly regulated insured depository institutions, credit unions already comply with a plethora of data privacy and security requirements, including the federal Gramm-Leach-Bliley Act (Public Law 106-102) and its implementing regulations, the California Financial Information Privacy Act (Cal. Fin. Code §4050, et seq.), and the National Credit Union Administration's (NCUA's) data security regulations (12 CFR Part 748 and its Appendixes).

B. Definition of a Business

The definition of a "business" subject to the requirements of the CCPA/CPRA requires further clarification.

- *Thresholds*

The CPRA changed the scope of covered businesses. Part of the definition of a business is that it satisfies one or more of the following thresholds:

> (A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
>
> (B) Alone or in combination, annually buys or sells, or shares the personal information of 100,000 or more consumers or households.
>
> (C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal Information.

The application of threshold (B) to the personal information of 100,000 or more "consumers or households" is confusing. A consumer, as defined in the CCPA/CPRA is a natural person California resident. Is the rest of the threshold then related to households of natural person California residents? Additionally, further clarification is needed to determine the method for counting the number of consumers or households toward the 100,000 threshold. For example, if one household has five individual residents/consumers, would they be counted as one (household), five (consumers) or six (five consumers plus one household) toward the 100,000 threshold?

- *Doing Business in California*

Another part of the definition of a business is that the entity "does business in the State of California." There is no clear definition under the CCPA/CPRA or the regulations of what it means to "do business" in the State of California. Clarification is needed.

For credit unions based outside of California, members may live in or relocate to California while maintaining a relationship with the out of state credit union through ATMs or a shared branching network. At what point does the non-California credit union become subject to the CCPA/CPRA despite the lack of a physical presence? "Doing business" in a state should mean something more than isolated or incidental transactions. There should be a clearly defined standard that contemplates intentional repeated and successive transactions that clearly indicates a pattern or practice of doing business with California consumers, and not one-time or occasional transactions.

C. GLBA and CFIPA Exemptions

The CPRA revised the CCPA's financial information exception to apply to "personal information collected, processed, sold, or disclosed ***subject*** to the federal Gramm-Leach-Bliley Act . . . , or the California Financial Information Privacy Act, . . . or the federal Farm Credit Act of 1971." (emphasis and revision added).

Regardless of this change, there is still significant confusion regarding the exemption for personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (CFIPA).

The confusion arises because the CCPA/CPRA uses terms that are inconsistent with the GLBA and CFIPA. The GLBA and CFIPA both use the terms "nonpublic personal information" and define that term to mean "personally identifiable financial information."

The CCPA/CPRA uses the term "personal information," which is defined in Calif. Civil Code §1798.140(o) and is much broader than the GLBA/CFIPA's definition of "nonpublic personal information."

In addition, the GLBA pertains to "personally identifiable financial information" collected in the course of a transaction or providing a financial product or service, etc. The CCPA/CPRA pertains to personal information collected in basically any manner, including when there is no transaction.

Because of the inconsistent terminology, the exemption provided in Calif. Civil Code §1798.145(e) is unclear and can be interpreted several ways. It is essential that the CPPA provide clarification in the regulations.

Moreover, for financial institutions that are only subject to the CCPA/CPRA notice requirements to the extent not covered by an exemption, guidance with regard to the appropriate response to a consumer that recognizes this exemption would be especially useful, given that consumers are unlikely to be familiar with the nature and extent to which the exemption applies.

D. Model Notices Needed

The CCPA and its regulations created several notice requirements, including:

- Notice at or Before Collection,
- Right to Opt-Out,
- Notice of Financial Incentives, and
- Updated Privacy Notices.

Further, the regulations require specific responses to certain verifiable consumer requests:

- Request to Know/Response, and
- Request to Delete/Response.

As noted above, the CPRA added the new right, the Right to Request Correction of Inaccurate Personal Information, which would require a specific response to another form of verifiable consumer request:

- Request to Correct/Response.

For all these required notices and responses, the regulations require the notices be easy to read and understandable by the average consumer and provide some standards to achieve that. This direction is subjective and does not contemplate a method or metric to assess the readability.

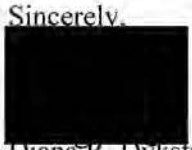
Since all businesses need to provide the required notices and responses, uniform model notices would help ensure consumer's understanding of the notices, simplify the requirements for businesses, and create an objective review on whether a business' notices meet the required standards. The Leagues recommend the CPPA draft proposed model notices for public comment and then include a safe harbor in the final regulations for the use of notices substantially similar to the model notices.

Final Comments

Ultimately, the League supports the spirit of the law and the need to protect the personal information of its members, but we continue to have significant concerns with the practicality and implementation of CCPA and CPRA.

We thank you for the opportunity to comment. We trust you will carefully consider our views and recommendations. If you have any questions regarding our comments, please contact me.

Sincerely,



Diana R. Dykstra
President and CEO
California Credit Union League

From: Kourinian, Arsen (Perkins Coie) [redacted]
Sent: 11/8/2021 4:01:27 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Shelton Leipzig, Dominique (Perkins Coie) [redacted]
Subject: PRO 01-21: CalChamber's Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020
Attachments: CalChamber - Comments on Proposed Rulemaking Under CPRA (PRO 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 Castanon,

Attached please find the comments of The California Chamber of Commerce in response to the California Privacy Protection Agency's September 22, 2021 Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21).

Please let us know if you have questions or any difficulty opening the document.

Best,

Arsen Kourinian | **Perkins Coie LLP**
GLOBAL PRIVACY COUNSEL – FIP, CIPP/US, CIPP/E, CIPP/C, CIPP/A & CIPM
[redacted]
F. +1.310.843.2805
[redacted]

20+ HOURS 2021 PRO BONO

PERKINSCOIE

1888 Century Park East
Suite 1700
Los Angeles, CA 90067-1721

+1.310.788.9900
+1.310.788.3399
PerkinsCoie.com

November 8, 2021

Dominique Regine Shelton Leipzig
[redacted]
F. +1.310.843.1245

Arsen Kourinian
[redacted]
F. +1.310.843.2805

VIA EMAIL

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

Re: Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (PRO 01-21)

Dear Debra:

Perkins Coie LLP hereby submits the following comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (CPRA) on behalf of The California Chamber of Commerce (CalChamber) (PRO 01-21). Comments are organized by the issues the California Privacy Protection Agency (the "Agency") raised as particular areas of focus in its invitation for preliminary comments: https://www.cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

COMMENTS

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

A. The Agency Should Limit the Scope of Cybersecurity Audits and the Risk Assessment to High-Risk Activities and to Prevent Bad Actors Getting Access to Business Data.

The Agency should place limits on cybersecurity audits and the risk assessment so that businesses can focus on high-risk activities, and to prevent bad actors from gaining access to business data that can be used to harm consumers.

Processing that presents a "significant risk to consumers' privacy or security," Cal. Civ. Code § 1798.185(a)(15), should be limited in scope to ensure that only high-risk and consequential activities are subject to a cybersecurity audit and the risk assessment. With regard to cybersecurity audits, it should be limited to data processing that, if compromised, is likely to result in tangible, concrete harms. For a privacy risk assessment, it should be limited to high-risk processing that has a legal or similarly significant effect. *See, e.g.*, Virginia Consumer Data Protection Act ("VCDPA") Va. Code § 59.1-576(A)(5); Colorado Privacy Act ("CPA") Colo. Rev. Stat. § 6-1-1309; European Union General Data Protection Regulation ("GDPR") 2016/679, Art. 35.

Processing tailored to protect consumers' privacy and security, such as processing for fraud prevention, anti-money laundering screening, or to otherwise comply with legal obligations, should be exempt from the scope of the risk assessment. *See* Cal. Civ. Code § 1798.145(1) & (5); Va. Code § 59.1-578(A)(7). These types of processing require confidentiality to prevent bad actors from gaining insight into internal systems. This approach will be beneficial for both businesses and consumers. For businesses, compelling them to divulge information in a risk assessment that can be used to exploit internal systems, threatens the critical security of information systems. Further, this approach will help protect consumers' personal information from being compromised because bad actors will not get additional information from businesses that they can use to breach consumers' personal information.

B. A Clear, Coherent Scheme of Audit and Risk Assessment Requirements with Other State Privacy Laws Will Streamline Consumer Privacy and Security.

Domestic and international privacy laws increasingly require businesses to conduct risk assessments and audits for certain high-risk processing activities. As the regulatory landscape expands, designing regulations to promote interoperability and consistency is critical.

The CPRA's risk assessment and audit regulations should align with existing California data security requirements (*see* Cal Civ. Code § 1798.81.5) and comparable state laws, such as the VCDPA (*see* Va. Code § 59.1-576(A)) and the CPA (*see* Colo. Rev. Stat. § 6-1-1309). The Agency should also accept risk assessments that were originally conducted pursuant to a comparable legal requirement and may consider accepting a summary of the type of risk assessment conducted and conclusions reached. Businesses that must conduct cybersecurity audits should be permitted to leverage existing certifications to make this process less onerous, such as 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; CIS Critical Security Controls; and/or security programs established pursuant to

consent decrees with regulators, such as the Federal Communications Commission or Federal Trade Commission ("FTC"). *See generally The Complete Guide to Understanding Cybersecurity Frameworks,* Dark Cubed, https://darkcubed.com/cybersecurity-frameworks.

The CPRA recognizes that a single risk assessment may address a comparable set of processing operations and may encompass the business's privacy program as a whole. Cal. Civ. Code § 1798.185(15)(B). Accordingly, the regulations should not require organizations to repeatedly conduct or submit a new risk assessment 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 medium-sized businesses that barely meet the CPRA's threshold and could incentivize businesses to treat a risk assessment as a mere "check-the-box" compliance exercise, which will not be helpful for protecting consumers' personal information.

The Agency should also ensure that a risk assessment remains confidential, and the rules should recognize that privileged information or trade secrets may be redacted. A risk assessment often includes sensitive information, including those relating to risk detection and risk mitigation processes. Permitting these processes to be released, such as through public inspection and copying under the California Public Records Act, Cal. Gov. Code § 6250 *et seq*, or otherwise, creates significant business and societal risks that are unjustifiable. For instance, releasing a risk assessment that relates to processing for fraud prevention, anti-money laundering screening, or compliance with other legal obligations can thwart their effectiveness by giving bad actors insights into internal systems, divulging information that can be used to exploit internal systems, or otherwise threatening the critical security of information systems. This in turn, creates the potential for even more risks to consumers through a state-disclosed roadmap for the potential breach of consumers' personal information. To avoid this, the regulations should clarify that risk assessments conducted pursuant to the CPRA are confidential and exempt from public inspection and copying under the California Public Records Act, Cal. Gov. Code § 6250 *et seq*. The Agency should also clarify that submitting a risk assessment pursuant to the CPRA does not waive attorney-client privilege or work product protections.

The Agency should further align the CPRA regulations related to a risk assessment so that they are consistent with existing legal requirements, including the GDPR, VCDPA, and the CPA. Alternatively, to help businesses better protect consumers' privacy across multiple jurisdictions, the Agency should also permit businesses to satisfy this obligation by complying with existing legal requirements under other states' laws (e.g., VCDPA and CPA) and applicable international laws (e.g., GDPR).

Lastly, the regulations should provide businesses flexibility to tailor risk assessment criteria as appropriate to the nature and risks of processing; regular submission of a generalized risk assessment should be periodic in nature.

C. Third-Party Auditor Mandates Unnecessarily Burden Businesses and Will Subject Consumers to Increased Expenses.

The regulations should recognize that any type of audit requirement will entail dedication of substantial personnel and financial resources to businesses. Consequently, to the extent that a business must complete cybersecurity audits on a periodic basis, the regulations should recognize that work performed in previous years remains relevant. The regulations could require that a business audit a single aspect of its cybersecurity program in a given year (e.g. vulnerabilities management or vendor management), or that a new audit only cover aspects of a cybersecurity program that have changed from one year to the next.

Businesses should have the option to choose between a third-party audit or an independent internal audit. Third-party auditors are disproportionately more expensive for businesses than independent self-audits. *See* Monique Magalhaes, *Cybersecurity Assessments and Audits,* TechGenix (Aug. 9, 2019), https://techgenix.com/cybersecurity-assessments-and-audits. Independent, internal self-audits facilitate transparency, while mitigating potential exposure of trade secret and proprietary information. Self-audit mechanisms that comply with appropriate industry standards, like PCI and NIST, should be sufficient to meet the CPRA's requirements. Notably, California law already contemplates processes for independent self-audits for the insurance industry, which the Agency can draw on. *See* Cal. Ins. Code. § 900.3. Businesses should also be able to leverage service providers' cybersecurity certifications and audits to help meet their own audit and risk assessment requirements. That said, the Agency should provide flexibility for businesses to choose whether an internal or external audit is suitable under the circumstances, instead of limiting businesses to one option.

2. Automated Decision-making.

A. Regulations Should Be Limited to Fully Automated Processing and to Critical Decisions.

We recommend that the Agency regulations for automated decision-making be limited to automated processes resulting in final decisions that have legal or similarly significant effects on consumers. Automated decision-making in processing activities is ubiquitous. Everyday technology like calculators, word processing software, and scantron machines could be considered automated decision-making technology. Even newer and more complex automated

decision-making technology, like artificial intelligence, is used routinely in business and includes things like email spam filters and autocorrect features. Arash Aghlara, *Decision Automation — What Is It and Why Should You Care*, Medium (Jan. 7, 2020) https://medium.com/decision-automation/decision-automation-what-is-it-and-why-should-you-care-637bda57974b.

The Agency's regulations for automated decision-making should be solely limited to automated processes resulting in final decisions that have legal or similarly significant effects on consumers. This approach will be beneficial for both consumers and businesses, as it will allow businesses to provide consumers faster and more streamlined services. Indeed, this approach will be consistent with other data privacy laws. *See e.g.*, GDPR, Art 15(1)(h) & 22(1); Colo. Rev. Stat. § 6-1-1306(1)(a)(C); Va. Code § 59.1-573(A)(5).

As discussed below in Section 2C, the CPRA does not grant consumers the right to opt-out of automated decision-making. Importantly, doing so is often infeasible and would result in numerous negative, unintended consequences. However, should the Agency require an opt-out for automated decision-making, it must be only under circumstances where the final decision-making is entirely automated, lacking human intervention, and results in legal or similarly significant effects. A corresponding access requirement to meaningful logic, if any, should similarly only apply to this category and should only consist of general criteria or categories of inputs used in reaching a decision, with protections for trade secrets.

Further, regulating only final business decisions is critical to enable businesses to serve consumers at scale. For example, individuals receive faster access to services if businesses can quickly identify low fraud risks. This is only possible at scale using either simple algorithms—e.g., approve transactions with no prior fraud flags—or more complex algorithms including ones using machine learning. Then, for the smaller set of fraud risk cases, businesses can use manual review to make final decisions, for example, through an appeals process. In these situations, if non-final decisions—e.g., cases flagged only by algorithms for further human review—are regulated, then consumers will receive slower access to services, and will incur higher costs from increased, and unnecessary, manual review. *See generally*, Mary Shacklett, *AI Decision Automation: Where It Works, and Where It Doesn't*, Tech Republic (Nov. 17, 2020), https://www.techrepublic.com/article/ai-decision-automation-where-it-works-and-where-it-doesnt. This approach would ensure that most activities relating to fraud prevention, abuse risk prevention, anti-money laundering processes, screening, or other types of security or compliance activities are generally not subject to restrictions that would render them less effective. *See* Va. Code § 59.1-578(A)(7).

B. Automation Is Core to Certain Services and Products, Rendering Opt-Outs Infeasible.

Automation may be core to certain high-risk service offerings that make opting-out infeasible. In these situations, it would be appropriate to provide businesses with an alternative to offering an opt-out right. For example, a safety system that automatically senses a car crash and immediately connects a user with assistance uses automation that is central to delivering the service. A user opting-out of the safety system would be contrary to the purpose for which they purchased a product because opting out would render the product useless.

In such instances, businesses should be able to demonstrate that they have operational guardrails that protect California consumers' interests instead of offering an opt-out right. Depending on the specifics of the use case, appropriate guardrails could include criteria such as rigorous testing under industry-standards, corroboration of results, ongoing monitoring, and appeals/complaint processes.

Additionally, the Agency should carve out processing related to fraud prevention, anti-money laundering processes, screening, and other security or compliance activities. *See* Va. Code § 59.1-578(A)(7). Failure to do so would, for example, enable bad actors from opting out of automated processes that detect and block their fraudulent activities, and limit companies' ability to protect consumers' privacy and security.

C. Automation Opt-Out Right Should be Confined to Rights Available Under the CPRA.

The CPRA expressly grants consumers the right to opt-out of the sale or sharing of their personal information and from certain uses of sensitive personal information. *See* Cal. Civ. Code §§ 1798.120 & 1798.121. The CPRA does not expressly grant consumers the right to opt-out of automated decision-making. Instead, it calls for regulations related to automated decision-making that are tethered to the CPRA's statutory rights of "access and opt-outs." *See* Cal. Civ. Code § 1798.185(a)(16). Since the CPRA does not create an express right to opt out of automated decision-making technology, the opt-out rights in this section are the express opt-out rights in the CPRA. In other words, the Agency is charged with considering how the opt-out rights expressly granted by the CPRA (i.e., sale/sharing and sensitive personal information) should relate to automated decision-making technology. *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 void as inconsistent with the authorizing statue Prop 57, because they denied some inmates consideration by the parole board to which they were entitled under Prop 57).

Thus, any attempt by the Agency to create an opt-out right beyond the express opt-out rights in the CPRA would be inconsistent with the authorizing statute and would also exceed the scope of the Agency's authority.

3. Audits Performed by the Agency.

A. Agency Audits Should Be Based on Evidence and Follow Transparent Legal Process with the Goal of the Agency and Businesses Working Together to Improve Privacy and Security, Instead of Threats of Enforcement Actions.

CPRA regulations related to Agency audits, Cal. Civ. Code § 1798.185(a)(18), should be based on lawful grounds and carried out through a transparent legal process. Being audited is an incredibly onerous task that takes time and resources away from the development of products and services that ultimately benefit consumers. To avoid audits from becoming random or arbitrary, the trigger for an Agency audit should be evidence that a business violated substantive provisions of the CPRA that harms or creates a substantial risk of harm to consumers.

The CPRA regulations should clarify the scope of the audit. The scope should be limited to addressing practices directly related to the misuse of personal information that necessitated the audit. Further, the purpose of the audit should be to help businesses improve their data privacy and security practices to better service consumers, instead of being part of the Agency's function of bringing enforcement actions. This will create an open and cooperative environment where the Agency and businesses will work together to improve privacy and security of data in California, instead of an adversarial relationship that will hinder such a beneficial partnership.

B. The Agency Should Perform Audits No More Than Once Every Three Years and Provide Adequate Notice.

To minimize the burden on businesses and the Agency, and to protect audits from becoming a tool for abuse, businesses should not be audited more than once in any three calendar years. Cal. Civ. Code § 1798.185(a)(18). In addition, the Agency should provide the business with at least 90 calendar days' notice prior to an audit. *Id.* Businesses need time to redirect internal resources to respond to and support audit requests. The business should also have the option to select an independent, certified auditor to perform any audits.

C. The Agency Should Protect Business and Consumer Information.

The Agency should formulate its audits to avoid access to or collection of consumers' information, unless absolutely necessary. Cal. Civ. Code § 1798.185(a)(18). Where the Agency does collect consumers' personal information, the Agency should be required to implement and document, as policy, appropriate technical and organizational measures to protect the data, including ensuring that it deletes the data when no longer needed for an Agency purpose.

By developing regulations consistent with these guideposts, it will help minimize creating any data security risks related to consumers' personal information and business data when businesses transmit such information to the Agency as part of the audit.

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

The Agency should develop CPRA regulations clarifying the scope of the CPRA right to correct and the corresponding business obligations arising from the same. *See* Cal. Civ. Code § 1798.185(a)(7) & (8).

A. Verification for the Right to Correct Should Be Permitted.

The Agency should extend existing CCPA regulations that require verifying the identity of a consumer before a business is obligated to honor a right to correct. *See* 11 C.C.R. §§ 999.323–999.326. Businesses should be able to develop processes to prevent fraud, such as by using the precise geolocation of a consumer to verify identity, or the staggering of time frames in which certain data is corrected. Businesses must be allowed to use strong methods of authenticating consumers' identities prior to releasing or changing personal information and should not be required to take extra steps to identify a consumer whose identity is unknown to the business. If the right to correct is not a verifiable consumer request, it could have significant consequences for consumers, as bad actors may try to alter consumers' information to steal their identity and assets.

B. Businesses Should Have the Option to Delete Inaccurate Data Where Appropriate.

Where appropriate, businesses should have the option to delete inaccurate data instead of replacing it with other data. For example, this is the approach taken under Canada's PIPEDA and the GDPR. Under PIPEDA, "[w]hen an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information . . . [through] the correction, ***deletion***, or addition of information." PIPEDA, S.C 2000, c. 5 Schedule

1(4.9.5) (emphasis added). Similarly, the GDPR states that controllers should ensure that inaccurate personal data is either "***erased or*** rectified without delay. . . ." GDPR art. 5(1)(d) (emphasis added).

Through this approach, businesses will have the option of removing outdated and inaccurate information from their systems, instead of correcting data that no longer serves a business purpose. Businesses will also advance the data privacy principles of data minimization and storage limitation by not only having such processes as a general business obligation, but also eliminating data from their systems that are brought to the business's attention by a consumer as being inaccurate. In sum, this flexible approach, consistent with PIPEDA and GDPR, will advance the data privacy and security of consumers and help businesses with their independent compliance obligations under general privacy and security standards and, specifically, under the CPRA. *See* Cal. Civ. Code § 1798.100(c) ("A business's 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, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.").

C. The Right to Correct Should Allow Businesses to Retain Evidence of Prior Inaccuracies.

The right to correct should allow companies to retain evidence of prior inaccurate information to comply with legal obligations and/or recordkeeping requirements. *See* Cal. Civ. Code § 1798.145(a)(1), (2), & (5); 11 C.C.R. § 999.317(d) ("A business's maintenance of the information required [for recordkeeping], where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.").

D. Businesses Should Be Allowed to Leverage Existing Processes for Correcting Personal Information.

The Agency should permit businesses to utilize their existing processes for correcting consumers' personal information, rather than creating new methods. This includes creating portals through which consumers can exercise their rights. This approach will be in line with the CCPA regulations, which, for example, permit businesses to verify a consumer's identity "through the business's existing authentication practices for the consumer's account," 11 C.C.R. § 999.324(a), and to use web portals to process consumer rights, *see id.* § 999.312(a) & (b).

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. A Universal Opt-Out Signal Should Be Developed with Industry Input.

There is uncertainty with any prospect of a universal opt-out signal because there are no guiding principles regarding its creation, implementation, universality, and the ability to reject it when the authenticity of the signal is in question. The universal signal should not be left to the devices of any single organization to create. It should be created with the required input from the industry so that no single entity exerts outsized influence over the signal's standards. Ideally there should be one signal. This would eliminate conflicting signals, and conflict among signals. This will further help businesses comply with emerging state laws that are also beginning to recognize opt-out signals, such as the CPA. *See* Colo. Rev. Stat. § 6-1-1306(a)(IV).

B. Opt-Out Signals Must Be Verified and Enable Consumer Choice Instead of Default Options.

Opt-out signals should apply only to recognized consumers and be applicable across browsers and devices. Opt-out signals should also allow consumers to opt-in and reverse any opt-out selection. *See* Cal. Civ. Code § 1798.135(b)(2). Opt-out signals must not come pre-set with default settings or be permitted to economize the sale of preferential default settings. Businesses should also have the right to notify consumers of the benefits and consequences of opting-out and the use of cookies. This will be critical so that opt-out signals truly "communicate or signal the consumer's choice to opt-out of the sale of their personal information," 11 C.C.R. § 999.315(c), instead of a default choice made for the consumer through pre-selected default browser options. *See* Cal. Civ. Code § 1798.135(b)(1) (stating that the opt-out signal should be "sent with the consumer's ***consent*** by a platform, technology, or mechanism. . . .") (emphasis added); § 1798.140(h) ("'Consent' means any ***freely given, specific, informed***, and unambiguous indication of the consumer's wishes. . . .") (emphasis added).

Indeed, an opt-out centralized through private actors at the browser or operating system level may create incentives for these companies to design and manage these controls in a way that harms competition or favors some businesses over others. Therefore, consideration should be given to mitigating such anti-competitive incentives.

C. Regulations on Opt-Out Signals Must Be Consistent with CPRA.

Regulations on opt-out signals 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. *See* Cal. Civ. Code § 1798.135(a) & (b)(1) ("A business shall not be required to comply with subdivision (a) if the business allows consumers to opt out . . . and to limit the use of their sensitive personal information through an opt-out preference signal. . . ."). Other consumer notice and competition considerations contained in Cal. Civ. Code § 1798.185(a)(19)(A) must also be reflected in the regulations.

Businesses should be limited to online data collection and should not be required to identify unauthenticated users to ensure that they are opted out of all forms of "sale" of personal information. Cal. Civ. Code § 1798.145(j) (stating that the CPRA shall not require "[r]eidentifying or otherwise link[ing] information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information").

6. Definitions and Categories.

A. The Definition of Dark Patterns Should Specify Focus on Fraudulent Practices.

The definition of "dark patterns" should be updated to focus on design practices that amount to consumer fraud. *See* Cal. Civ. Code § 1798.140(l). Specifically, the definition currently focuses on whether the dark pattern subverts or impairs people's autonomy, decision-making, or choice. *Id.* But there is no empirical way to assess whether the interface impairs people's autonomy or choices. The current definition would have the unintentional consequence of prohibiting privacy-protective default settings because they would impair choice and autonomy.

Thus, the CPRA definition of "dark patterns" is overinclusive because 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 thus specify that the definition of "dark patterns" is focused on design practices that amount to consumer fraud. 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, and it should align with the rich body of FTC case law, which turns on

whether the misrepresentation or omission is material. Federal Trade Commission, Enforcement Policy Statement Regarding Negative Option Marketing, Oct. 28, 2021.

Sincerely,

[redacted]

Dominique Regine Shelton Leipzig

DRSL:mcj

cc: Arsen Kourinian
Megan Von Borstel
Naa Kai Koppoe
Shoeb Mohammed

From: Jaime Huff [redacted]
Sent: 11/8/2021 4:36:24 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21: CJAC Comments on Preliminary Rulemaking
Attachments: CJAC Comments CCPA Regulations Submitted on 11-8-21.pdf

[EXTERNAL]: [redacted]

Dear CPPA Staff -

Attached please find CJAC's comments regarding the preliminary rulemaking by the California Privacy Protection Agency.

If you have any questions don't hesitate to reach out to me at [redacted].

Thank you,
Jaime

Jaime R. Huff
Vice President and Counsel, Public Policy
Mobile [redacted] | www.cjac.org
CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

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,

[redacted]

President and Chief Executive Officer

---

[10] Cal. Civ. Code § 1798.150(b).

From: Wolkowitz, Rachel [redacted]
Sent: 11/8/2021 3:04:19 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Rachel Sanford Nemeth [redacted]; Douglas Johnson [redacted]
Subject: PRO 01-21: Consumer Technology Association comments on the CPPA Invitation for Comments
Attachments: CTA comments to CPPA (12.8.21)-c3.pdf

[EXTERNAL]: [redacted]

Ms. Castanon:

Please find attached comments of the Consumer Technology Association ("CTA") in response to the Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 by the California Privacy Protection Agency.

Please reach out with any questions.

Thank you,
Rachel Wolkowitz
Counsel for CTA

WILKINSON BARKER KNAUER LLP

Rachel S. Wolkowitz
1800 M Street, NW
Suite 800N
Washington, DC 20036
Tel: [redacted]
Main: 202.783.4141
[redacted]
www.wbklaw.com

Before the
CALIFORNIA PRIVACY PROTECTION AGENCY
Sacramento, CA 95814

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

COMMENTS OF
CONSUMER TECHNOLOGY ASSOCIATION

I. INTRODUCTION

Consumer Technology Association ("CTA")® respectfully submits these comments in response to the Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 ("Invitation for Comments") by the California Privacy Protection Agency ("Agency" or "CPPA").[1] As North America's largest technology trade association, CTA® *is* the tech sector. Our members are the world's leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES® – the largest, most influential tech event on the planet. CTA and its members thus have a substantial interest in the CPRA, the CPPA and related implementing regulations.

CTA urges that any regulations the CPPA ultimately adopts be necessary, timely, risk-based and implementable by business, including small businesses. In addition, the regulations should not create more barriers for consumers to access the services they want, whether in the form of onerous consents, more complicated notices or more costly products.

---

[1] Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020, Proceeding No. 01-21 (Sept. 22, 2021) ("Invitation for Comments"). In approving Proposition 24, California voters adopted the California Privacy Rights Act of 2020 ("CPRA"), which amended and extended the California Consumer Privacy Act of 2018 ("CCPA") and established the California Privacy Protection Agency ("Agency").

Since the CCPA was signed into law two and a half years ago, companies of all sizes subject to CCPA's requirements have raced to establish processes, policies and systems to come into compliance with the law and then related regulations adopted by the Attorney General. For many companies, particularly small businesses that have invested significantly in systems to come into compliance with Europe's General Data Protection Regulation ("GDPR"), as well as U.S.-focused businesses not subject to the GDPR that had not yet deployed new data governance processes and systems, building CCPA-compliant programs already has been a substantial, challenging and expensive initiative. Companies are now in the process of building programs to comply with the CPRA amendments, as well as with the state privacy laws adopted in Colorado and Virginia. In the absence of a federal, comprehensive privacy law, CTA urges the CPPA to ensure that any regulations the Agency adopts are harmonized with other state requirements as discussed herein. Below, CTA first sets forth general principles to guide the CPPA's approach to developing regulations, then describes how to approach the unique challenges of automated decisionmaking ("ADM") and finally provides more specific comment on certain individual topics.

II. LIMITING REGULATIONS TO REQUIREMENTS THAT IMPOSE THE LEAST BURDEN NECESSARY ON BUSINESSES WILL MAXIMIZE RESULTS FOR CONSUMERS AND INNOVATORS

CTA encourages the CPPA to champion a balanced, flexible and technology-neutral privacy framework. Agency regulations should be necessary, timely, risk-based, harmonized and implementable by businesses, including small businesses. Such regulations should maintain consumers' trust while also allowing innovation that relies on the use of data collected from consumers. They should also build on existing protections and requirements already in California's statutes and regulatory code as well as existing standards.

Necessary. These regulations should not create more barriers for consumers to access the services they want, whether in the form of frequent consents, more complicated disclosures, or more costly products. Privacy regulation should provide legal clarity while maintaining the flexibility to innovate. Indeed, to the extent businesses can maintain the flexibility to innovate, both in terms of the products they provide and the data security and privacy protections they can offer, consumers will benefit from best-in-class technology. Red tape imposed in the name of privacy could prevent innovative companies from proving their technologies and services in the marketplace. Any regulation should be targeted to enable companies to maximize resources to drive meaningful privacy protections for consumers.

Timely. For practices that are dynamic and evolving, the Agency should not rush to adopt new one-size-fits-all rules. For example, with respect to ADM, as discussed in more detail below, the Agency should take a risk-based approach to govern potential transparency and opt-out requirements. ADM tools are new technologies that many private and public sector actors, including regulators, are only now beginning to understand. Rather than move too quickly, the Agency should use this rulemaking process to develop a robust record that accounts for technological changes and that balances risks versus the benefits of overregulation.

Risk-Based. Privacy regulation should focus on the type of data at issue, recognizing that sensitive data may warrant heightened protections, rather than specific technologies or industry sectors, because, as explained by CTA's President and CEO Gary Shapiro, "not all data is equally sensitive."[2] With the CPRA, California voters enshrined numerous additional rights and requirements in statute; the Agency should be sure that regulatory requirements are materially

[2] Gary Shapiro, *We Need a Federal Privacy Law – Not a Patchwork of State Laws*, Morning Consult (May 6, 2019), https://morningconsult.com/opinions/we-need-a-federal-privacy-law-not-a-patchwork-of-state-laws.

benefiting consumers and mitigating demonstrable risks, rather than merely generating paperwork.

Harmonized. Consistent protections across technologies, companies, agencies and state borders are a bedrock prerequisite to ensure consumer trust, continue data-driven innovation and realize its benefits. The CPPA should seek to harmonize regulations and leverage existing, successful practices, where possible, such as with the Virginia and Colorado privacy law, where definitions – like those around sensitive personal data – are emerging and represent consumer expectations. Further, the Agency should leverage published and familiar standards, such as utilizing National Institute of Science and Technology ("NIST") controls[3] in the cybersecurity audit context.[4] Such standards have been vetted by experts, policymakers and industry and have been proven effective.

Keeping the above principles as lodestars for potential regulation will maintain consumers' trust while also allowing innovation that relies on the use of data collected from consumers.

III. THE AGENCY SHOULD PROCEED CAUTIOUSLY TO DEVELOP A ROBUST RECORD AND NARROWLY TAILORED REGULATIONS REGARDING AUTOMATED DECISIONMAKING

ADM tools enabled by machine learning and related processes are new technologies that many private and public sector actors, including regulators, are only now beginning to understand. Given the nascent nature of this technology and the novel questions of law and policy presented in the Invitation for Comments, the CPPA should proceed cautiously. Further,

[3] *See, e.g.*, National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5 (September 2020).

[4] *See* Invitation for Comments Topic 1(b) (seeking comment on the nature of cybersecurity audits).

the statute does not define key ADM terms and there is no legislative history on which to rely.[5] As a result, the CPPA is left to construe ambiguous terms and concepts that involve emerging/evolving technologies. For these reasons, the Agency should proceed only after developing a robust record. As explained below, any regulations that the CPPA develops regarding ADM should be tailored to cover only those decisions having legal effect (or similarly consequential effect), require clear consumer disclosures when necessary to protect legal or consequential rights and include narrowly framed opt-out rights.

A. The Scope of "Covered Automated Decisionmaking Technology" Should be Narrow and Focused Only on Those *Decisions* Having Legal (or Similarly Consequential) Effect

The CPPA wisely raises general scoping and definitional questions at the outset, asking what activities should fall within the scope of ADM technology and profiling.[6] CTA suggests that rather than focusing on automated decision-making *technology*, any new regulations that may come out of this process should focus on automated *decisions* that lack human direction. This approach aligns with other privacy laws, which focus on specific uses of and rights related to decisions based on automated processes rather than on the *technologies* used to arrive at those decisions.

Also, the scope of any new duties around ADM technology should be limited to only those fully automated decisions that lack human direction and that produce a direct and

[5] The statute does not define key concepts, such as "automated decision-making technology," "opt-out" or "meaningful information." In fact, the statutory language does not provide for an opt-out right; this concept is only found in the section relating to regulations. The lack of a statutory definition reaffirms the need for a deliberate and thoughtful process to address fundamental questions about scope, definitions and intent related to this rulemaking process.

[6] Invitation for Comments Topic 2(a) (seeking comment on what activities constitute "automated decisionmaking technology" and/or "profiling").

immediate legal effect (or similarly consequential effect) on individuals.[7] Such decisions are properly subject to heightened scrutiny and could be within scope.[8] However, many ADM decisions are not consequential (either legally or otherwise) and should be excluded from the scope of potential regulation. For example, many systems provide recommendations or decisions about music, video, products or online content, while other systems review standardized tests, manage industrial systems or perform other similar functions that enable autonomous systems. Clearly, decisions arising in these situations are not of legal effect and should be excluded from any potential new rules.

In addition, some automated decisions, including profiling, when used to maintain the safety, integrity and security of online or automated services should be excluded from scope.[9] Also, any automated decisions that are used in autonomous vehicles, systems and transportation should be excluded, as those systems do not produce decisions of legal effect and are clearly outside scope. Further, ADM tools used for internal analytics, communications or performance evaluation within any enterprise (and not applied to consumers) should be outside of scope. Finally, the CPPA should exclude the many online services using ADM decisions to provide services and content that subscribers explicitly request. Automated recommendations enable

---

[7] This standard aligns with recently enacted statutes in Virginia and Colorado, both of which provide an opt-out for profiling that is "in furtherance of decisions that produce legal or similarly significant effects" concerning the consumer.

[8] This narrowly tailored approach is similar to the scope of affected automated decision systems addressed in California AB 13, a bill introduced in the California legislature. The bill focuses on "high-risk application[s]" of ADMs that involve "a score, classification, recommendation, or other simplified output," that support or replace human decision-making, in situations that "materially impact a person." *See* California AB-13 (version as amended by California Senate on July 15, 2021), https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB13&showamends=false.

[9] For example, such companies may rely on these kinds of automated decisions to display age-appropriate content to younger users or identify and de-prioritize problematic content.

personalization, which is the basis for a wide variety of free and paid online services that consumers specifically request.

B. Consumers Should Have Access to Information About ADM Decisions When Necessary to Protect Legal or Consequential Rights of Affected Individuals

The CPPA's Invitation for Comments seeks input on the question of when consumers should be able to access information about the use of ADM.[10] As explained above, consumers should be able to access information about the use of ADM technology when businesses use that technology to make decisions that have direct and immediate legal effect (or similarly consequential effect) on an individual. This standard is consistent with recently enacted laws in Virginia and Colorado and provides a useful framework for deciding when consumers' rights to information arise. Further, limiting this right to those circumstances where the legal effect is "direct and immediate" provides both a temporal and causation test to ensure that individuals do not seek information or raise claims about ADM decisions that do not have a direct causal relationship to the individual, or which are attenuated from a timing perspective. In other words, consumers should not be able to request information about ADM decisions that are older than twelve months, or which have no direct causal relationship to the consumer's legal rights.

C. Covered Providers Should Provide Clear, High-Level Information About the Use of Automated Decisionmaking Consistent with Standards for Explainable AI Recently Released by NIST

CTA agrees that in certain cases some information about how automated decisions are made should be provided to consumers.[11] This obligation should only arise when automated

---

[10] Invitation for Comments Topic 2(b) (When should consumers be able to access information about the use of ADM technology? What process should be used to facilitate such access?).

[11] Invitation for Comments Topic 2(c) (What information should be provided in response to consumers' access requests, including the scope of "meaningful information about the logic" involved in ADM decisions?).

decisions have direct and immediate legal or similarly consequential effects on an individual. Providing some level of transparency with respect to such automated decisions is consistent with the statutory mandate and helpful to consumers.

However, transparency obligations should be calibrated to provide clear, high-level information about the use of ADM to make certain decisions, and the type of data used to make the decision. With respect to the scope of "meaningful information about the logic" involved in ADM decisions, a flexible standard that accounts for the type of data used and the processes used by the ADM system should be considered. Under this approach, covered entities would be required to: (1) inform the individual affected of the type of data their algorithms use and, (2) explain in plain language how the algorithm makes decisions. Explanations of how the algorithm makes decisions must be meaningful, i.e., accessible and stated in plain terms to ensure they can be easily understood by the general public.

Any attempt to mandate greater granularity in such explanations could lead to the development of less accurate algorithms. Indeed, the more variables an algorithm uses in a model, the more complex that model becomes and the more difficult it is to provide meaningful explanations about the decision.[12] This leads to a tradeoff between accuracy and interpretability. While it may be appropriate to require certain ADM decisions that present a high-risk to provide greater details, a one-size-fits-all rule that applies broad mandates to all ADM decisions should

[12] *See* Nick Wallace and Daniel Castro, *The Impact of the EU's New Data Protection Regulation on AI*, Center for Data Innovation, at 10 (Mar. 27, 2018), https://www2.datainnovation.org/2018-impact-gdpr-ai.pdf ("*The Impact of the EU's New Data Protection Regulation on AI*").

be avoided. In any event, the CPPA should not mandate detailed disclosures that could undermine the accuracy of ADM systems.[13]

Transparency obligations should also reflect other important considerations, such as technical feasibility, trade secrets and consumer information overload. In some cases, it simply may not be technically feasible to provide detailed, individualized explanations for all automated decisions. For example, this may be true in highly complex interrelated systems used in autonomous vehicles. Nor should transparency obligations supersede any organization's right to keep confidential trade secrets, intellectual property or other confidential and proprietary information. Finally, the degree of transparency obligations should take in to account the amount of information that ordinary persons may be able to understand or process.

ADM is also an area where the CPPA should leverage the work of other expert agencies. In particular, NIST recently released a White Paper on "explainable" AI that provides a useful framework to consider human-machine interaction.[14] Importantly, NIST's explainable AI principles were developed based upon a comprehensive public record and process of public consultation, and its principles support the provision of meaningful, accurate and knowledge-limited explanations. The White Paper acknowledges that "[e]xplanations in practice will vary, and should, according to the given system and scenario. This means there will be a large range of ways an explanation can be [] embedded into a system."[15]

---

[13] Further, the CPRA does not provide any right to delete or correct data used in ADM tools. The CPPA should therefore avoid adoption of any new mandates that would require data deletion or correction in association with the issues discussed herein.

[14] *Four Principles of Explainable AI*, NISTIR 8312 (Sept. 2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf; *see also* https://www.nist.gov/artificial-intelligence/ai-fundamental-research-explainability.

[15] *Id.* at 3, Sec. 2.1.

The CPPA should look to the NIST White Paper to provide aligned guidance with what businesses must do to provide "meaningful information about the logic" involved in the ADM process. With respect to providing "meaningful information" NIST emphasizes contextual variability that does not lend itself to a one-size-fits-all approach: "what is considered meaningful will vary according to the explanation's purpose"[16] in part because "[d]ifferent scenarios and needs will drive what is important and useful in a given context."[17] Thus, context is key and variability is essential when considering the scope and nature of explanations in this context.[18]

Moreover, the industry is working to develop appropriate principles and best practices to ensure this technology is used fairly and appropriately. CTA and others in the tech industry are working to create a "trust framework for AI" that will enhance transparency and user rights. For example, CTA has been active in examining AI-related issues, publishing standards and research papers intended to forge common understandings of AI's role in society and terms used in the AI discourse.[19] The CPPA need not regulate where industry initiatives are ongoing.

Any attempt to proscribe regulations dictating specific transparency or explainability standards risks missing the mark. Instead, the Agency should consider general principles, like those articulated by NIST, to guide the industry toward adoption of best practices and principles

---

[16] *Id.* at 4, Sec. 2.2.

[17] *Id.*

[18] Notably, there is no suggestion in the NIST White Paper that the actual logic, or underlying code or algorithm, of the automated decisionmaking system should be disclosed. Such information is confidential and proprietary, and must be recognized as such.

[19] *See, e.g.*, Riya Andandwala and Danielle Cassagnol, CTA, Press Release, CTA Launches First-Ever Industry-Led Standard for AI in Health Care (Feb. 25, 2020) https://www.cta.tech/Resources/Newsroom/Media-Releases/2020/February/CTA-Launches-First-Ever-Industry-Led-Standard; CTA Definitions and Characteristics of Artificial Intelligence (ANSI/CTA-2089), Feb. 2020, https://shop.cta.tech/collections/standards/products/definitions-and-characteristics-of-artificial-intelligence (defining terms related to artificial intelligence and associated technologies).

that will facilitate the exchange of meaningful and accurate information with affected consumers. A top-down, one-size-fits-all form of explanation will serve neither consumers nor the industry.

D. Consumers' Opt-Out Rights Should be Narrowly Framed and Available After a Showing That the Consumer Is Likely to Face a Significant Adverse Decision with Direct and Immediate Legal Effect

The CPPA should carefully consider whether opt-out rights offer any tangible benefit before considering any new rules around such rights.[20] While Europe has maintained an ADM opt-out right under its overarching privacy law – the GDPR – a recent UK Taskforce on Innovation, Growth and Regulatory Reform has asked whether the UK should eliminate this right from the country's data protection regime.[21] This raises questions about the efficacy of such a right.

Should the CPPA decide to proceed with developing regulations to provide such rights, then opt-out rights should be limited to those situations involving fully automated decisions that produce a significant adverse decision that is direct, immediate and which has legal effect (or similarly consequential effect) on the individual, and where there is no human oversight or involvement in the decision. Limiting the scope of opt-out rights is necessary to ensure that the costs of compliance do not become overwhelming, and to avoid loss of the utility and accuracy of the ADM tool itself.

Article 22 of the GDPR is similarly limited in scope and subject to certain exceptions.[22] For example, the right to opt out does not apply when the automated decision is necessary for

---

[20] Invitation for Comments Topic 2(d) (seeking comment on the scope of consumers' opt-out rights with regard to automated decisionmaking, and what processes consumers and businesses should follow to facilitate opt outs).

[21] *See* Department for Digital, Culture, Media & Sport, *Data: A new direction, Public Consultation On Reforms To The UK's Data Protection Regime*, https://www.gov.uk/government/consultations/data-a-new-direction (rel. Sept. 10, 2021).

[22] *See* GDPR, Art. 22(2).

entering into or executing a contract involving the data subject. The right also does not apply if the automated decision is authorized by a law of the EU or EU Member State, so long as the law includes suitable safeguards to protect the data subject's interests. Further, the opt-out right does not apply when the automated decision is based on explicit data subject consent.

Providing opt-out rights necessarily means that the humans will be required to review the ADM decision and come to a separate decision based upon the same data used by the ADM tool. However, human review of ADM decisions is costly, inefficient and can lead to ill-informed decisions. The Center for Data Innovation has explained that "there is a trade-off between the representational capacity of a model and the ease with which a human can review the calculations it makes."[23] This is so because as models gather and analyze more data they become more complex, and the insights generated from such models become more difficult to replicate or analyze. It takes a human more time to analyze and process large amounts of data which an ADM tool can process in seconds.

Consider also that decisions made by humans are not without potential bias or inaccuracy. Indeed, some evidence exists that human decisions are often less accurate and more susceptible to bias than algorithmic decisions.[24] Nor are humans always transparent or well-equipped to explain their decisions. Humans are disposed to providing incomplete, inaccurate or inconsistent decisions or explanations and "are prone to misunderstanding and misremembering their own subjective experience of the world."[25] Therefore, providing opt-out rights to enable human review of significant adverse decisions of legal effect is often of limited utility.

---

[23] *The Impact of the EU's New Data Protection Regulation on AI* at 9.

[24] *Id.* at 11.

[25] *Id.*

Finally, any opt-out right from ADM decisions should exclude applications in which humans work with automated systems, including human-machine collaborations and human-developed processes working alongside the ADM. For example, Alexa and other "smart home" systems communicate prompts that are transmitted back to human technicians. The human operators review transmitted messages to improve the product's algorithms and safeguard consumer rights by monitoring the performance of the Alexa system.[26] Clarifying the definition of "automated decisionmaking" in this way will protect the interests of consumers by creating clear expectations for all parties.

IV. COMMENTS ON SPECIFIC TOPICS

A. Processing of Personal Information that Presents a "Significant Risk to Consumers' Privacy or Security"

As the Agency considers what regulations are appropriate to address businesses' processing of personal information that could present significant risk to consumers' privacy or security, including submission of risk assessments, it should look to the Virginia Consumer Data Protection Act as a model for relevant criteria.[27] Specifically, under the Virginia law, such assessments identify and weigh the potential direct and indirect benefits of processing for the controller, consumer, other stakeholders and the public against the risks to the consumer, as mitigated by relevant safeguards. In addition, the analysis should include the use of deidentified data, the reasonable expectations of consumers and other contextual details. This will allow the CPPA, individuals and businesses with a clear and comprehensive picture of the risks that they must anticipate and manage.

---

[26] *See, e.g.*, Amazon Alexa Privacy Hub, https://www.amazon.com/b/?node=19149155011&ref=ap_ing (last visited Nov. 8, 2021).

[27] Invitation for Comments Topic 1(c); Virginia Consumer Data Protection Act § 59.1-576.

In terms of implementing any regulations, the CPPA should make clear that a risk assessment submitted to the Government is confidential and exempt from public inspection and copying under California's Freedom of Information Act. Likewise, the CPPA should set up a similar protection for any other data, algorithms and material that the agency is authorized to review. Once a business has completed and submitted a risk assessment, a business should not be required to perform additional risk assessments unless there has been a material change in the processing of personal information.[28]

B. Annual Cybersecurity Audits

Any guidance or rules to implement the CPRA annual cybersecurity requirement should be (i) focused on security outcomes and (ii) flexible enough to allow companies to remain agile and adopt best practices and new security solutions, as they emerge.[29] As noted in Section II, with respect to cybersecurity audits, the Agency should leverage published and familiar standards in cybersecurity audits such as NIST controls.[30] Industry and policymakers have developed these standards into effective tools that are already well-known and utilized. NIST also provides a useful assessment & auditing resources page for entities implementing the NIST Cybersecurity Framework.[31] The Agency should consider making available similar resources to provide a starting point for companies, especially small businesses. Businesses should not be required to use any particular resource, though.

---

[28] *See* Invitation for Comments Topic 1(c) (seeking comment on how often businesses should have to submit risk assessments).

[29] *See id.* Topic 1(b) (seeking comment on the nature of cybersecurity audits).

[30] *See, e.g.*, National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5 (September 2020 (includes updates as of Dec. 10, 2020)).

[31] National Institute of Standards and Technology, Cybersecurity Framework - Assessment & Auditing Resources (last updated January 12, 2021), https://www.nist.gov/cyberframework/assessment-auditing-resources.

C. Consumer Right to Correct

The CPRA introduced a right to request correction of inaccurate personal information to help consumers control personal data. When setting out procedures and limitations on requests to correct, the CPPA should adopt similar procedures to the existing CPPA rights on deletion and access to help provide both individuals and businesses with clarity and set expectations appropriately.[32]

The new right to correct also raises difficult operational challenges as data is processed among entities. The Agency can help mitigate these challenges by requiring that 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 and shared by another party. A business that was not the original source of the information should be able to direct the consumer back to the original source so that the information is corrected once and for all. This places the responsibility on the party best in position to correct the inaccurate data without sweeping in entities that cannot effectively carry forth the consumer's wish to correct their data.

D. Consumer Request to Know

As noted in the Invitation for Comments, when businesses are required to disclose specific pieces of information to a consumer, the CPRA generally requires the disclosure to cover the 12 months prior to a consumer's request.[33] However, for all information processed on, or after January 1, 2022, consumers may request, and businesses must disclose, information

[32] *See* Invitation for Comments Topic 4 (seeking comment on regulations implementing a consumer's right to correct).

[33] Invitation for Comments Topic 7.

beyond the 12-month window, subject to certain exceptions.[34] Providing such information should be considered "impossible" or to "involve a disproportionate effort" if it is not readily available and in electronic format.[35] For example, a business that has information in archive systems or non-electronic formats should be exempt from providing such information beyond the 12-month window.

V. CONCLUSION

CTA urges the CPPA to develop regulations that do not impose significant compliance burdens or cause operational challenges to companies, without any commensurate privacy benefit to consumers. To guard against such burdens without benefits, the Agency requirements should be consistent with those under other privacy regimes, timely, risk-based and implementable. Such a regime will provide both important protections for consumers and the flexibility needed to innovate.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Rachel Nemeth*
Rachel Nemeth
Senior Director, Regulatory Affairs

/s/ Douglas K. Johnson
Douglas K. Johnson
Vice President, Emerging Technology Policy

1919 S. Eads Street
Arlington, VA 22202
[redacted]

November 8, 2021

[34] *Id.*

[35] *See Id.* Topic 7(a).

From: Stacey Gray [redacted]
Sent: 11/8/2021 4:58:49 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Jules Polonetsky [redacted]; John Verdi [redacted]
Subject: Future of Privacy Forum Comments, PRO 01-21
Attachments: Future of Privacy Forum Comments PRO 01-21.pdf

[EXTERNAL]: [redacted]

Good evening,

Thank you for the invitation to submit preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020.

Please see the attached comments on behalf of the Future of Privacy Forum.

Regards,
Stacey Gray

--

Stacey Gray
Senior Counsel
Future of Privacy Forum
[redacted] www.fpf.org | 1400 Eye Street NW, Suite 450, Washington, DC 20005

Subscribe to our monthly newsletter!

FUTURE OF PRIVACY FORUM

1400 Eye Street NW, Suite 450, Washington, DC 20005 | 202-768-8950 | fpf.org

November 8, 2021

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

RE: Future of Privacy Forum Comments, PRO 01-21

Dear Ms. Castanon and Members of the California Privacy Protection Agency,

The Future of Privacy Forum (FPF) welcomes this opportunity to weigh in on initial rulemaking under the California Privacy Rights Act. FPF is a 501(c)(3) non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Our primary office is in Washington, DC, and we work closely with our colleagues in Brussels, Singapore, Tel Aviv, and around the world. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation.[1]

In response to the Agency's invitation for comments, and with regard for the particular categories of information requested,[2] we offer resources and recommendations below regarding: automated decisionmaking, sensitive personal information, global opt-out signals, and de-identification.

Regulations under the California Privacy Rights Act should:

1. Establish guidelines for automated decisionmaking (ADM) that produces "legal or similarly significant effects."
2. Provide that information about "automated decisionmaking" follow NIST interpretability guidelines, and be meaningful and reasonably understandable to the average consumer.
3. Clarify a range of potential use cases for health and wellness data, by providing a principled, exemplar list of categories that are in or out of scope. In many cases, such distinctions will be based on context and reasonable use.
4. Ensure opportunities for socially beneficial commercial research using sensitive personal information.
5. Clarify the role of global opt-out signals in the context of today's labyrinth of existing permission frameworks, including in authenticated and non-authenticated platforms.
6. Establish an open process for authoritative approval of new global opt-out signals that meet the technical specifications of the Agency over time.

---

[1] The views herein do not necessarily reflect the views of our supporters or Advisory Board.
[2] 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.

7. Seek further input from de-identification experts and researchers to clarify key implementation issues for "deidentified data," including the role of technical, legal, and administrative controls, and Privacy Enhancing Technologies (PETs).

Part A. Automated Decisionmaking - 1798.185(a)(16)

1798.185(a)(16) requires the Agency to issue regulations governing access and opt-out rights with respect to the use of automated decisionmaking (ADM) technologies, including profiling. Although the CPRA does not specifically regulate automated decisionmaking (ADM), the concepts are useful for the purposes of understanding CPRA consumer rights (access, deletion, opt-out of sale and sharing, and limiting the use of sensitive personal information).

In general, we recommend that the Agency craft user controls to: (1) address the potential for harms caused by automated decisionmaking when it leads to "legal or similarly significant effects" on consumers, including clarifying when the use of sensitive personal information may be "necessary to perform the service or provide the goods reasonably expected by an average consumer" to identify and address bias and discrimination in high-risk decisions. Regulations should also provide (2) that information about "automated decisionmaking" follow NIST interpretability guidelines, and be meaningful and understandable to the average consumer.

1. Regulations should establish guidelines for automated decisionmaking (ADM) that produces "legal or similarly significant effects."

Strictly interpreted, "automated decisionmaking" encompasses almost every form of modern technology. This includes many routine, low-risk practices, such as loading a website, email filtering, or providing content recommendations.[3] However, some commercial automated decisions present serious risks to individual rights and autonomy, particularly in areas such as hiring, tenant screening, insurance, and other risk scoring.[4] Many of the most serious use cases fall outside the scope of CPRA (e.g., AI used in criminal sentencing, or by HIPAA-covered entities to make diagnosis decisions).

In order to distinguish higher risk automated decisionmaking from the broader world of all technology that involves "automation" (that is, all technology), a helpful guidepost would be to

[3] For a relevant comparison, the federal government maintains a list of automated processes in its Robotic Process Automation Use Case Inventory, providing detailed information on over 300 RPA Use Cases across the federal government. *See* U.S. General Services Administration, Federal Robotic Process Automation (RPA) Community of Practice, RPA Use Case Inventory, https://digital.gov/pdf/federal-rpa-use-case-inventory-compliant.pdf.

[4] *See, e.g.*, Miranda Bogen and Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias* (Dec. 2018), Upturn, https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

align the CPRA regulations with Article 22 of the GDPR by applying heightened protections to automated decisions that lead to "legal or similarly significant effects."[5] The standard "legal or similarly significant effects" has the benefit of capturing high-risk use cases, while encouraging interoperability with global frameworks, for which a growing amount of legal guidance is becoming available.

According to leading guidance in the European Union,[6] decisions with "legal effects" include decisions that affect a person's legal rights, such as those that result in the cancellation of a contract, or entitlement to or denial of a benefit granted by law. "Similarly significant effects" includes decisions that do not necessarily alter a legal right, but have a similarly substantial impact on individuals, including in their circumstances and life opportunities. Commonly cited examples include: automatic refusal of an online credit application; decisions made by online job recruitment platforms; and decisions that affect other financial, credit, employment, health, or education opportunities.[7]

While the GDPR directly limits such processing (by prohibiting most "solely" automated decisionmaking that leads to legal or similarly significant effects), the statutory text of the CPRA likely does not offer such tools. Nonetheless, within the parameters of the law, California regulations can still create meaningful, workable safeguards for individuals. For example, regulations can clarify that:

- Automated decisionmaking (ADM) that leads to legal or similarly significant effects on consumers, can be subject to data protection impact assessments[8] to identify benefits and mitigate risks to consumers, per 1798.185(a)(15)(B)); and
- Businesses engaged in automated decisionmaking that leads to legal or similarly significant effects should have systems in place for identifying and addressing bias and discrimination, even in cases where such analysis may conflict with other rights. For example, the consumer right to "Limit the Use of Sensitive PI" applies generally to the use of any sensitive personal information under the CPRA, whether or not it involves automated decisions. Businesses seeking to address bias in automated decisionmaking may make inferences about race, ethnicity, or other sensitive information. In such cases,

---

[5] Art. 22 GDPR.
[6] European Data Protection Board, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (Oct 2017), https://ec.europa.eu/newsroom/article29/items/612053.
[7] In some cases, the Article 29 Working Party has noted that online advertising may be considered to have similarly significant effects under the GDPR, for example if it is particularly intrusive, targets vulnerable populations or uses knowledge of the vulnerabilities of individuals. This could include, for example, targeting "someone known or likely to be in financial difficulties . . . with adverts for high interest loans."
[8] This requirement exists in the GDPR. Art. 22 GDPR. Models for risk assessments include, for example: UK Information Commissioner's Office, Sample DPIA Template (Feb. 2018), https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf; FPF, Mobility Data Sharing Assessment (Aug. 2021), https://fpf.org/blog/fpf-and-mobility-data-collaborative-release-resources-to-help-organizations-assess-the-privacy-risks-of-sharing-of-mobility-data/.

regulations can encourage the development of accountability by clarifying that such uses are necessary to perform the service when high-risk decisions are involved.

2. **Regulations should provide that information about "automated decisionmaking" follow NIST interpretability guidelines, and be meaningful and reasonably understandable to the average consumer.**

1798.185(a)(16) also requires the Agency to establish rules for how businesses should comply with consumer access rights, when they involve automated decisionmaking. Access to information about the logic or functioning of an automated decision is most typically sought for decisionmaking that involves so-called "black box" algorithms in realms with high impact on consumers, such as in loan approval, hiring, or insurance. In developing regulations on this topic, California should follow NIST interpretability guidelines,[9] and require that responses to access requests be meaningful and understandable to average consumers.

Both the challenges and the need for providing meaningful information about AI-driven decisionmaking are not new. The Equal Credit Opportunity Act (ECOA)[10] and the Fair Credit Reporting Act (FCRA)[11] mandate customer-level explanations known as "adverse action notices" for automated decisions in the consumer finance space. Similarly, Article 22 of the GDPR requires businesses to "provide meaningful information" about the logic involved in automated decisionmaking about individuals that leads to legal or similarly significant effects.

In practice, however, it can be a challenge to provide truly meaningful, explainable, or interpretable AI for average consumers. Instead, what most consumers want to understand are the factors that led to a high-impact decision, and the main reasons for it. For example, in the case of an algorithmic decision tree for approval or denial of a loan: it is not enough to provide only "input data" (factors such as credit score and income) and "output" (in this case, approval or denial). In order for that information to be meaningful, a business would likely also need to share information about the relative salience (weight) of each factor. More complicated AI systems, such as neural networks, present an even greater challenge in situations where they are used to impact significant consumer decisions.

We recommend that California follow best practices and guidance from NIST's "Four Principles of Explainable Artificial Intelligence" (2020),[12] which articulates principles for explainable AI systems: "that the system produce an explanation, that the explanation be meaningful to humans, that the

---

[9] P. Jonathon Phillips et. al, *Four Principles of Explainable Artificial Intelligence*, U.S. Department of Commerce, National Institute of Standards and Technology (August 2020), https://www.nist.gov/system/files/documents/2020/08/17/NIST%20Explainable%20AI%20Draft%20NISTIR8312%20%281%29.pdf.

[10] Equal Credit Opportunity Act, 12 C.F.R. § 1002.9(a)(2).

[11] Fair Credit Reporting Act, 15 U.S.C. § 1681m.

[12] *See*, supra note 9.

explanation reflects the system's processes accurately, and that the system expresses its knowledge limits."

Further Resources:

- P. Jonathon Phillips et. al, *Four Principles of Explainable Artificial Intelligence*, U.S. Department of Commerce, National Institute of Standards and Technology (August 2020), https://www.nist.gov/system/files/documents/2020/08/17/NIST%20Explainable%20AI%20Draft%20NISTIR8312%20%281%29.pdf.
- European Data Protection Board, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (Oct. 3, 2017), https://ec.europa.eu/newsroom/article29/items/612053.
- *Explainable AI*, IBM, https://www.ibm.com/watson/explainable-ai.
- Aaina Agarwal, Patrick Hall, Sara Jordan, and Brenda Leong, *Five Things Lawyers Need to Know About AI* (October 2021), https://fpf.org/blog/five-things-lawyers-need-to-know-about-ai/.
- FPF, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning* (October 2018), https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf.

Part B. Sensitive Personal Information - 1798.185(a)(19)(C)

1798.185(a)(19)(C) requires the Agency to issue regulations to "govern the use or disclosure of a consumer's sensitive personal information, notwithstanding the consumer's direction to limit the use or disclosure of [such information]." The CPRA enables consumers to direct businesses to limit the use of 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."

3. **Regulations should help clarify a range of potential use cases for health and wellness data, by providing a principled, exemplar list of categories that are in or out of scope. In many cases, such distinctions will be based on context and reasonable use.**

The CPRA's inclusion of heightened protections for "sensitive personal information" aligns with trends in the European Union, and extends current protections in the United States for medical and health condition information.[13]

Regulations should help clarify the scope of this new category with respect to a range of potential use cases for commercial health and wellness data:

[13] The Federal Trade Commission has so far provided the strongest legal protections for commercial non-HIPAA health information in the United States. *See, e.g.*, Federal Trade Commission, *Flo Health, Inc.*, https://www.ftc.gov/enforcement/cases-proceedings/192-3133/flo-health-inc (involving improper disclosure of user data from fertility tracking apps).

- ***Diagnoses and medical conditions.*** Direct information about a consumer's medical diagnosis or health condition, such as an illness or injury, should be considered clearly within scope.
- ***Commercial data used to provide health-related products and services.*** Commercial data used to infer characteristics about a person's health should likely also be considered in-scope. For example, electronic medical record data, information traditionally subject to the FTC Health Breach Notification Rule,[14] or data collected through the use of consumer products that allow individuals to monitor vital signs (smart thermometer, glucose monitors, pulse oximeters, EKG app, etc.) would all be in scope. Similarly, health websites and apps that collect information with the intent to contact individuals about medications, or that request user reported health information (e.g. blood sugar, eating habits, or sleep patterns) and subsequently provide advice on health conditions or possible diagnoses would be considered sensitive.
- ***Fitness and wellness data.*** Regulations should clarify whether commercial wellness data, unrelated to a particular health condition or diagnosis (and not used for that purpose), is or is not in scope. For example, many health and fitness apps track information such as steps, workouts, meditation sessions, diet, or lifestyle information. Absent analysis of this data and generation of inferences regarding health conditions or diagnoses, this information is most appropriately categorized as non-sensitive.
- ***Inferences, educated guesses, and proxies.*** Finally, regulations should clarify that deliberate, sensitive inferences based on information that would otherwise be out of scope should be included as "sensitive personal information," based on its use for that purpose, regardless of accuracy. For example, social media, web search, browsing, or music/video streaming data, should likely all be considered out of scope generally. However, it should be clear that a business would be brought back in scope for limiting the use of "sensitive personal information" if it were to use such data to generate a health-related inference, such as to provide a targeting category of "likely to have X condition." In some cases, sensitivity will depend on context. For example, body characteristics such as height and weight may or may not "concern health," depending on use (e.g., to generate a BMI score, or, for example, to adjust a vehicle's safety settings).

Broadly speaking, "health" includes a wide range of potential information, and clarification here will be valuable. The CPRA already makes a useful distinction with respect to sensitive personal information based on context and use. Specifically, sensitive PI that is "collected or processed without the purpose of inferring characteristics about a consumer" is exempted from the opt-out requirement in Section 1798.121. We recommend that this distinction be applied broadly to the extent that sensitive categories of PI are treated differently in other areas of the law, such as the right to access (Section 1798.110), and restrictions on incompatible secondary use (Section 1798.100). In addition to the businesses' "purpose," the regulations should also consider reasonable context and risks to consumers.

[14] FTC Health Breach Notification Rule, 16 C.F.R. § 318.3 (2021).

4. **Regulations should ensure opportunities for socially beneficial commercial research using sensitive personal information.**

Finally, regulations should clearly encourage socially beneficial commercial research, including where it must be balanced against the consumer's right to access and delete information. For example, it may be beneficial for large platforms to conduct research on the effect of their services on consumers' mental health or time spent using online services. Similarly, businesses that provide direct-to-consumer health and wellness services may be continuously generating new health inferences, within ranges of potential accuracy. In some cases, it could be concerning, or even unethical, to inform individuals about low-confidence or ongoing health inferences, even while the research itself proves useful and could lead to new health breakthroughs in the future.

Notwithstanding the above, exempting data from access and deletion requirements for purposes of research should not allow for businesses to retain sensitive information for non-research purposes, for example if they are selling or disclosing data to third parties for marketing or other non-research purposes.

Part C. Opt-Out Signals - 1798.185(a)(19)

1798.185(a)(19) requires the Agency to issue regulations to define the requirements and technical specifications for opt-out preference signals sent by a platform, technology, or other mechanism. We support this and recommend that it serve as an opportunity to establish strong standards that will clarify and streamline options for consumers, and shape the adoption of similar tools in other jurisdictions. California should (1) clarify the role of opt-out signals in the context of today's labyrinth of existing permission frameworks; and (2) establish an open process for approval of new global opt-out signals that meet the specifications of the Agency over time.

5. **Regulations should clarify the role of global opt-out signals (i.e., not just one signal) in the context of today's labyrinth of existing permission frameworks, including in authenticated and non-authenticated platforms.**

In a fragmented data ecosystem, the adoption of universally accepted signals, including through user agents such as browsers or plug-ins, has become a practical necessity for individuals to control data collection. Without such signals, or other limits on data collection, opt-outs create an unworkable burden on individuals to identify, and individually contact, hundreds of commercial entities that might or might not process their data. It has been well documented that this is

unnavigable for average, and even very sophisticated, consumers.[15] Against this backdrop, the adoption of global opt-out signals in California, whether mandated[16] or voluntary and incentivized,[17] is a significant step forward.

However, the same fragmentation that compels adoption of global opt-out signals, has led to a mass of confusion for individuals and businesses who attempt to navigate sometimes conflicting opt-outs, settings, and signals. Today, consumers have a complicated web of options to express preferences and exercise some form of control over the sale, sharing, or use of personal information in mobile, web, and offline environments. The current volume of choices is largely unnavigable, yet relied upon by many businesses across sectors for legal, policy, and technical reasons. The confusion reflects decades of platform, business, and self-regulatory efforts to address privacy concerns without the underpinning of a single, comprehensive privacy law.

As an illustration, the options below exist today to control: browser and device-specific data; data within authenticated platforms; and offline or "physical world" information. Each of these cases raises unique issues for the adoption of global opt-out signals, which California should address through rulemaking to simplify and streamline existing systems for consumers and businesses.

***Browser and device-specific data*:**

Existing browser and device-specific controls include: privacy settings (to block cookies, block third-party cookies, "prevent cross-site tracking"); browser plug-ins; global signals such as Do Not Track or the Global Privacy Control; and self-regulatory mechanisms such as NAI Consumer Opt Out and DAA YourAdChoices. Similarly, control over mobile apps can be exercised through device settings (iOS and Android), including "Limit Ad Tracking," and app-specific permissions.

- ***Issue***: A business with browser or device-specific data (such as a cookie ID, or IDFA) may or may not be readily able to link that data to data from the same consumer on a different browser or device, or to traditional personal information processed separately.
- ***Recommendation***: Regulations should clarify that a global opt-out request associated with less readily available data (such as a cookie ID, browser information, or IDFA) should apply to the sale of all data with which the opt-out signal can be reasonably linked.

***Authenticated platforms*:**

Large and small platforms and businesses that have direct relationships with consumers increasingly offer their own "privacy dashboards" with settings for various uses of data occurring

---

[15] Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, Consumer Reports & Digital Lab (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf; Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society, Vol. 4, No. 3 (2008), *543-568*, https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.

[16] Cal. Code Regs. tit. 11 § 999.315 (Requests to Opt Out).

[17] CPRA Section 1798.135.

on and off-platform. These include settings for: social media; retail; financial institutions; educational services; and consumer technology (e.g., Smart TVs, vehicles, or children's toys).

- ***Issue***: Any business with a direct consumer relationship must navigate possible conflicts between the known privacy settings of their users, and global opt-out signals received from devices that may or may not belong to their users.
- ***Recommendation***: Regulations should clarify what steps a platform should take when it receives a device or browser-specific global opt-out signal from (1) a consumer who has an account with the business and is authenticated (logged in); (2) a consumer who has an account with the business, but is not authenticated (not logged in); and (3) a consumer who does not have an account with the business.

"Offline" or "physical world" information:

As the average consumer's number of devices grows, there is a growing industry for analyzing and using passive information sent by networked devices, or inferred from external behavior and appearance. Opt-outs sometimes include modifying device settings at the point of collection (such as MAC address randomization[18]), but more often are self-regulatory and limited in scope. Many opt-out mechanisms do not currently exist, or have yet to be developed (e.g., for video analytics, facial recognition, and augmented reality).

- ***Issue***: Global opt-out signals for offline data collection are largely limited in scope or do not yet exist.
- ***Recommendation***: Regulations should anticipate the development of such signals, and provide guidance for how to shape them. For example, California could encourage the widespread adoption of an SSID-based signal such as "_nomap" for the broader location industry that relies on network information within the control of individuals.[19] California could also encourage the development of user agents to control offline and Internet of Things (IoT) data.[20]

California should establish practical guidelines for businesses to navigate complex permissions systems, in a way that will simplify and streamline the current confusion for consumers.

6. **California should establish an open process for authoritative approval of new global opt-out signals that meet the technical specifications of the Agency over time.**

In a fragmented world of web, mobile, screenless IoT, and emerging technologies, there can rarely or never be "one opt-out signal to rule them all," at least without a corresponding trade-off in anonymity and privacy. New tools will continue to be developed. Each of them, like the controls

[18] *See, e.g.*, Apple Support, "Use private Wi-Fi addresses on iPhone, iPad, iPod touch, and Apple Watch," https://support.apple.com/en-us/HT211227 (last visited Nov. 8, 2021).
[19] *See, e.g.*, Google Maps Help, "Control access point inclusion in Google's Location services" (last visited Nov. 8, 2021), https://support.google.com/maps/answer/1725632?hl=en.
[20] *See, e.g.*, The Personalized Privacy Assistant Project, https://privacyassistant.org/.

and signals above, will necessarily function as a *partial* opt-out: applying to a certain kind of data, within a certain realm of processing.

As technology and business practices continue to evolve, under heightened pressure from platform rules and privacy regulation, it is likely that many more opt-out and consent tools will emerge. California should establish an open, authoritative process for approval of global opt-out signals that will be deemed to adhere to California law. We recommend that the Agency do so in consultation with technical, legal, and policy experts, as well as leaders in other jurisdictions that are developing similar tools, such as Colorado. In addition to granting businesses the benefit of clarity, consumers deserve to know which tools they choose will have legal effect.

In addition to a principles-based approach to establishing criteria for global opt-out signals (we agree, for example, that signals and opt-out tools should be easy-to-understand, and not contain defaults that misalign with the law[21]), the process should create procedural opportunity, for example by allowing civil society organizations or members of the public to propose new opt-out signals (their own or otherwise), allow stakeholders to weigh in, and involve a deliberative process that evaluates the many technical and policy factors in alignment with the Agency's criteria, such as: scale of adoption; alignment with criteria in other jurisdictions; and the extent to which the signal is possible to localize solely to consumers in California.

Part D. De-Identified and Pseudonymous Data - 1798.185(a)(2)

1798.185(a)(2) requires the Agency to issue regulations to update, as needed, the definitions of "deidentified" and "unique identifier" to address changes in technology, data collection, obstacles to implementation, and privacy concerns.

The CPRA defines "deidentified" as:

> "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business . . . (A) takes reasonable measures to ensure that the information cannot be associated . . . (B) publicly commits to maintain and use the information in deidentified form . . . and (C) contractually obligates any recipients of the information to comply with all provisions of this subdivision." 1798.140(m).

While this language aligns with the longstanding approach of the Federal Trade Commission,[22] there remains little guidance or enforcement activity to help organizations understand how

[21] CPRA 1798.185(a)(19).
[22] U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012).

"deidentified" will be interpreted by regulatory authorities in California. There are several key issues related to the interpretation and implementation of de-identification tools within the U.S., including California, that would benefit from greater certainty.

7. **Regulations should seek further input from de-identification experts and researchers to clarify key implementation issues for "deidentified data," including the role of technical, legal, and administrative controls, and Privacy Enhancing Technologies.**

We recommend that the Agency convene further specialized input, including through meetings and workshops, from leading de-identification experts, as well as researchers with experience using de-identified data safely. Public input, regulations, sector-specific guidance, and enforcement actions can serve to clarify key global issues related to de-identification, specifically:

- what constitutes "reasonable" measures to ensure that the information cannot be associated with a consumer or household;
- the status of certain types of protected, pseudonymized information, in which personal information is no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures[23]; and
- technical measures needed to make de-identified data legally public under the CPRA.[24]

Evaluating privacy risk in de-identified data requires specialized, case-by-case assessments that consider a range of technical and contextual factors, which are often sector-specific. However, businesses often lack the internal expertise and capacity to deploy PETs in effective ways.[25] Although there are a growing number of vendors and practitioners offering such services, the availability of qualified PETs experts is extremely limited nationwide. By providing guidance on these topics, the Agency has an important opportunity to incentivize businesses' use of PETs to support the utility of data while mitigating risks to consumers.

Further Resources:

- NIST, *NISTIR 8053: De-Identification of Personal Data* (Oct. 2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

---

[23] See, e.g., Patrick Breyer v Bundesrepublik Deutschland, Judgment of the Court (Second Chamber) of 19 October 2016, https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN.

[24] CPRA requires businesses processing deidentified data to "contractually [obligate] any recipients of the information to comply with all provisions of this subdivision." 1798.140(m). Greater clarity would be helpful with respect to how this provision applies to de-identified information released to the general public.

[25] For example, differentially private methods can be effective in providing mathematically sound guarantees of privacy, reflected by an epsilon value that indicates re-identification risk, sometimes called a "privacy budget." However, limited guidance exists to determine what these values should be for different contexts or types of data. See, e.g., Alexandra Wood, et al, *Differential Privacy: A Primer for a Non-Technical Audience*, 21 Vanderbilt J. Ent. & Tech. L. 209, 260 (2018), https://dash.harvard.edu/bitstream/handle/1/38323292/4_Wood_Final.pdf?sequence=1.

- Miranda Mourby et. al, *Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK*, Computer Law & Security Review, Volume 34, Issue 2 (Apr. 2018), 222-233, https://www.sciencedirect.com/science/article/pii/S0267364918300153.
- Khaled El Emam, Eloise Gratton, Jules Polonetsky, and Luk Arbuckle, *The Seven States of Data: When is Pseudonymous Data Not Personal Information?*, https://fpf.org/wp-content/uploads/2016/11/El-Emam_States-of-Data-Main-Article-short-v6.pdf.
- FPF, *A Visual Guide to Practical Data De-Identification* (June 2017), https://fpf.org/wp-content/uploads/2017/06/FPF_Visual-Guide-to-Practical-Data-DeID.pdf.
- Jules Polonetsky, Omer Tene, and Kelsey Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara L. Rev. 593 (2016), https://digitalcommons.law.scu.edu/lawreview/vol56/iss3/3/.
- Claire McKay Bowen, *Personal Privacy and the Public Good: Balancing Data Privacy and Data Utility*, Urban Institute (August 2021), https://www.urban.org/sites/default/files/publication/104694/privacy-and-the-public-good_0_0.pdf.

Thank you for this opportunity to provide input on initial rulemaking under the California Privacy Rights Act. We welcome any further opportunities to provide resources or information to assist in this important effort.

Sincerely,

Stacey Gray, *Senior Counsel*

Jules Polonetsky, *CEO*

Future of Privacy Forum
1400 Eye St. NW Ste. 450
Washington, DC, 20005
info@fpf.org

FUTURE OF PRIVACY FORUM

From: Shapiro, Tracy [redacted]
Sent: 11/8/2021 4:39:58 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Holman, Eddie [redacted]
Subject: PRO 01-21
Attachments: WSGR Response to Invitation for Preliminary Comments on Proposed Rulemaking Under the CPRA (PRO 01-21).pdf

[EXTERNAL]: [redacted]

Dear Board Members and Staff of the California Privacy Protection Agency:

Attached please find our comment on the proposed rulemaking under the California Privacy Rights Act of 2020.

Sincerely,

Tracy Shapiro

WILSON SONSINI

Tracy R. Shapiro | Partner, Privacy & Cybersecurity | Wilson Sonsini Goodrich & Rosati
One Market Street | San Francisco, CA 94105 [redacted]

WILSON SONSINI

Wilson Sonsini Goodrich & Rosati
Professional Corporation
One Market Plaza
Spear Tower, Suite 3300
San Francisco, California 94105-1126
O: [redacted]
F: 415.947.2099

TRACY R. SHAPIRO
Internet: [redacted]
Direct dial: [redacted]

EDDIE HOLMAN
Internet: [redacted]
Direct dial: [redacted]

November 8, 2021

Board Members and Staff
California Privacy Protection Agency
915 Capital Mall, Suite 350A
Sacramento, CA 95815

Re: Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (PRO 01-21)

Dear Board Members and Staff of the California Privacy Protection Agency:

Wilson Sonsini Goodrich & Rosati appreciates the opportunity to submit these comments in response to the California Privacy Protection Agency's invitation for preliminary comments on its proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA). We submit these comments on behalf of certain of our clients, including companies that provide security and fraud prevention services and companies that purchase online advertising, though to be clear, these comments do not necessarily reflect the views of all of our clients. These companies appreciate the importance of consumer privacy and data protection, and we submit these comments with the aim of encouraging the Agency to issue regulations that will protect the privacy of consumers in a manner that is effective, practical, and allows companies to continue to provide consumers with valuable services.

General Comment Regarding Harmonization of Privacy Laws

Many U.S. companies have adopted global privacy programs in which they aim for a high-water mark in protecting consumers' personal information and empowering consumers with control over how their personal information is processed. They have already invested significant resources in these programs in response to the California Consumer Privacy Act (CCPA), EU General Data Protection Regulation (GDPR), and other federal, state, and global privacy laws and regulations, and will soon need to adjust these programs to address the CPRA, the Virginia

Consumer Data Protection Act (VCDPA),[1] the Colorado Privacy Act (ColoPA),[2] and any other state privacy laws that may soon be enacted. We therefore encourage the Agency to seek to harmonize the CPRA regulations with other privacy regimes to avoid conflicting laws and to ease companies' compliance burdens wherever possible.

To provide a few examples, companies' compliance burdens will increase to the extent that:

- Privacy laws contain competing definitions or interpretations of terms such as personal information and sensitive information;
- In order to comply with various U.S. state privacy laws, companies must implement different processes for responding to access and deletion requests, including if those laws contain conflicting exceptions for when companies need not respond to such requests; or
- Requirements for service provider or contractor agreements conflict with other states' requirements.

For the Right to Correct, the Agency should adopt common sense limitations on this right, similar to those relating to the GDPR right to rectification, such as allowing businesses to decline to allow individuals to amend personal information: (a) where the information is subjective in nature; (b) in order to protect the rights or freedoms of other data subjects; (c) where the request would obstruct an investigation or legal proceeding; or (d) where the request is manifestly unfounded or excessive. Further, the Agency should clarify that the consumer's Right to Correct personal information does not apply to data that a business uses to train machine learning algorithms, to the extent that those algorithms will not produce legal effects or similarly affect the consumer. As discussed by the UK Information Commissioner's Office, the purpose of training data is to train models based on general patterns in large datasets, so the individual inaccuracies are less likely to have any direct effect on an individual data subject.[3]

We also encourage the Agency to implement CPRA regulations that are consistent with the CCPA regulations where possible, as companies have spent significant resources to develop compliance programs around them. For example, consistent with the CCPA, the processes for the verification of requests should stay the same and consumers' right to delete should include an exemption for data stored in archives and backups. Conversely, CCPA regulations that are inconsistent with the CPRA and the Agency's rulemaking instructions, such as Section 999.315(c) of the existing CCPA regulations, should be immediately repealed until they can be replaced with

---

[1] Va. Code § 59.1-575 to -585.

[2] Colo. Rev Stat. § 6-1-1301 to -1313.

[3] Reuben Binns, *Enabling Access, Erasure, and Rectification Rights in AI Systems*, UK ICO AI Blog (Oct. 15, 2019), https://ico.org.uk/about-the-ico/news-and-events/ai-blog-enabling-access-erasure-and-rectification-rights-in-ai-systems/.

new regulations consistent with the CPRA's requirements so as to avoid wasting resources complying with regulations that lack a statutory basis.

Comments Responding to Agency's Topics for Public Comment

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

1.a: Businesses' processing of personal information for security and integrity purposes does not present a "significant risk to consumers' privacy or security."

Section 1798.185(a)(15) requires businesses to annually conduct cybersecurity audits and submit to the Agency risk assessments if their processing of personal information poses a significant risk to consumer's privacy and security. The processing of personal information solely for security and integrity purposes does not pose a significant risk to consumers' privacy or security, and therefore should not trigger Section 1798.185(a)(15)'s requirements. "Security and integrity" is defined by the CPRA to include the ability to detect security incidents, prevent malicious, fraudulent, or illegal activities, and protect people's physical safety.[4] By definition, this type of processing promotes, rather than jeopardizes, consumer security and privacy. Indeed, if processing a consumer's personal information for security and integrity purposes presented a "significant risk to consumers' privacy or security," then the cybersecurity audit required by Section 1798.185(a)(15) may itself create that risk, creating a circular analysis that may have the net effect of reducing overall security practices by businesses seeking to avoid conducting costly audits. Accordingly, processing consumer personal information for these purposes should be exempted from Section 1798.185(a)(15)'s audit and risk assessment requirements. Businesses would benefit from clarification by the Agency that this type of processing is not considered a significant risk to consumers and will not trigger Section 1798.185(a)(15)'s requirements.

1.b: Businesses required to conduct cybersecurity audits and submit risk assessments should be permitted to meet these requirements by submitting certificates of widely accepted audits.

Businesses that are covered by Section 1798.185(a)(15)'s cybersecurity audit and risk assessment requirements should have the option of satisfying these requirements by providing the Agency with certificates of widely accepted cybersecurity audits and risk assessments (e.g., ISO 27001 certificate or certificate of third-party audit or SOC 2 audit). This approach enables the Agency to gain visibility into the sufficiency of businesses' security practices while avoiding the disclosure of details about businesses' information security programs, networks, and infrastructure that may be useful to a threat actor. Further, many businesses already engage in risk assessments and audits as part of a robust information security program. Requiring them to undertake an additional risk assessment and audit specifically for CPRA compliance purposes

[4] *See* Cal. Civ. Code § 1798.140(ac).

would result in a duplication of effort and may be prohibitively expensive for many businesses with no meaningful benefit to consumers.

2. ***Automated Decisionmaking***

2.a: The definitions of "profiling" and "automated decisionmaking" should be tied to activities that impact individuals' rights.

The Agency should adopt regulations that limit the access and opt-out rights provided under Section 1798.185(a)(16) to "profiling" or "automated decisionmaking" that affects a legal right or has a similar significance. In its current form, the CPRA's definition of "profiling" may be unworkably broad.[5] By narrowing the definition or applying any associated access or opt-out rights in such a way that they apply only to profiling that affects a legal right or has similar significance, businesses can focus on building consumer access processes and opt outs for the most important types of processing: those that have potentially significant impacts on individuals' rights. Conversely, forms of profiling and automated decisionmaking that provide benefits to or are unlikely to harm consumers may continue.

Further, this approach would harmonize the CPRA with other privacy regulations. The GDPR, for example, contains a limitation similar to the one suggested above. Article 22 of the GDPR—which addresses profiling and automated decisionmaking—provides that data subjects "have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[6] Similarly, the ColoPA provides Colorado consumers with the right to opt out of the processing of personal data concerning the consumer for the purposes of "[p]rofiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer."[7] The Agency should incorporate equivalent language into its definitions of "profiling" and "automated decisionmaking."

2.a-d: The processing of personal information solely for purposes of security and integrity should not be considered "profiling" or "automated decisionmaking" that would trigger access or opt-out rights.

Processing consumers' personal information for security and integrity purposes should not be considered "profiling" or "automated decisionmaking" that would trigger the access or opt-out rights under Section 1798.185(a)(16). Many companies that we work with offer or utilize

---

[5] *See* Cal. Civ. Code § 1798.140(z) (defining "profiling").

[6] *See also* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L. 119) 1, 14 (Recital 71).

[7] Colo. Rev Stat. § 6-1-1306(1)(a)(I).

services that employ automated measures to help safeguard network security and consumers' personal information. Automated processes play a critical role in companies' ability to detect and prevent malicious threats, fraud, and illegal activity.

Requiring businesses to provide the public with details about the automated processes used in security and integrity processing will undoubtedly weaken the efficacy of those measures. Section 1798.185(a)(16) provides that "access" in this context "include[s] meaningful information about the logic involved in those decisionmaking processes." Threat actors and fraudsters will no doubt exploit this requirement to gain information needed to evade security controls and fraud detection measures.

Moreover, this access provision may require businesses to disclose trade secrets relating to the proprietary automated logic, systems, and processes they use to implement security measures. The Agency has authority under Section 1798.185(a)(3) to adopt regulations "[e]stablishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights . . . with the intention that trade secrets should not be disclosed in response to a verifiable consumer request." The Agency should use this authority to clarify that any access right provided in Section 1798.185(a)(16) does not require companies to divulge trade secrets or other intellectual property.

Businesses should also not be required to provide an opt out to automated decisionmaking related to security and integrity. Bad actors would take advantage of this requirement to circumvent the controls designed to improve security and detect fraud.

For the reasons stated above, we request that the Agency clarify in its regulations that processing for security and integrity purposes does not qualify as "profiling" or "automated decisionmaking" that would trigger an access or opt-out right under Section 1798.185(a)(16).

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***

5: The Agency should provide guidance on the definition of "cross-context behavioral advertising."

The Agency should provide guidance on the scope of "cross-context behavioral advertising." With the CPRA's current definition, we expect the Agency will likely take the position that consumers have a right to opt out of having businesses share their personal information with advertising technology providers that use the data to build consumer segments or profiles for ad targeting by other advertisers. In contrast, if a business shares a consumer's personal information for contextual advertising, such as where the advertising technology provider shows the consumer an ad based on the consumer's search or the content viewed, that would not constitute cross-context behavioral advertising.

Nevertheless, there are numerous forms of online advertising that do not fall neatly into these two buckets. For example:

- a business may make available a consumer's personal information to an ad tech provider in order to retarget ads to that consumer. The business may prohibit the provider from building segments or otherwise using the data for the provider's own purposes or on behalf of other advertisers, but the provider may still need to use some of its own data about the consumer to effectuate the retargeting;

- a business may use its existing customers' personal information in order to not target ads to them as part of an ad campaign; or

- a business may use existing customers' personal information in order to create so-called "lookalike audiences" and target ads to similar consumers.

While, in our view, these types of advertising activities do not constitute cross-context behavioral advertising, businesses would benefit from more certainty regarding the Agency's opinion on these common advertising arrangements.

We recognize that it would not be realistic for the Agency to address every form of online advertising in its regulations. Nonetheless, businesses would benefit from additional color regarding what it means to target 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." Without additional clarification, businesses will interpret this language differently from one another, resulting in inconsistent treatment when consumers exercise their right to opt out.

5.b: Recommendations for Opt-Out Preference Signals

Subsequent to the passage of the CPRA, the state of Colorado passed its own general privacy law, the ColoPA, which takes effect on July 1, 2023. Like the CPRA, the ColoPA creates certain opt-out rights for Colorado residents, which have some overlap with, but are not identical to, consumer opt-out rights under the CPRA. Specifically, the ColoPA provides Colorado consumers with the right to opt out of the processing of personal data (as defined by the ColoPA) concerning the consumer for purposes of:

1. "Targeted advertising," i.e., displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests, subject to certain exceptions;[8]

[8] Colo. Rev Stat. § 6-1-1303(25).

2. The "sale" of personal data, i.e., the exchange of personal data for monetary or other valuable consideration by a controller to a third party, subject to certain exceptions;[9] and/or

3. Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.[10]

Of these three opt-out rights, the ColoPA further directs the Colorado Attorney General to "adopt rules that detail the technical specifications for one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data."[11]

The CPRA, on the other hand, provides California residents with substantively different opt-out rights. Specifically, the CPRA gives California residents the right to:

1. Opt out of the "sale" or "sharing" of personal information, subject to certain exceptions;[12] and/or

2. Limit the use and disclosure of sensitive personal information, subject to certain exceptions.[13]

The CPRA further directs the Agency to issue "regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling,"[14] potentially creating a third opt-out right. Of these opt-out rights, Section 1798.185(a)(19)(A) directs the Agency to issue "regulations to define the requirements and technical specifications for 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 and to limit the use or disclosure of the consumer's sensitive personal information." To enable this opt-out preference signal, Section 1798.185(a)(19)(A)(vi) requires that consumers be presented with up to three choices, including:

> (I) Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information.

---

[9] Colo. Rev Stat. § 6-1-1303(23).

[10] Colo. Rev Stat. § 6-1-1306(1)(a)(I).

[11] Colo. Rev Stat. § 6-1-1313(2).

[12] Cal. Civ. Code § 1798.120.

[13] Cal. Civ. Code § 1798.121.

[14] Cal. Civ. Code § 1798.185(a)(16).

(II) Choice to "Limit the Use of My Sensitive Personal Information."

(III) Choice titled "Do Not Sell/Do Not Share My Personal Information for Cross Context Behavioral Advertising."

With this background in mind, we recommend the Agency undertake the following in creating the CPRA regulations:

1. **Section 999.315(c) of the existing CCPA regulations should be immediately repealed.** The regulations' current requirement that businesses "treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device 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 submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer" is inconsistent with the requirements for an opt-out preference signal under Section 1798.185(a)(19), which is already in effect. In particular, the current requirement does not require that the signal be free of defaults, as required by 1798.185(a)(19)(A)(iii), nor does it make honoring the signal optional, as clearly required by Section 1798.135(b)(3) of the CPRA.

   Because of these fundamental inconsistencies and to avoid the unnecessary expenditure of resources by businesses to comply with a regulatory requirement that conflicts with the text of the statute, the Agency should immediately repeal Section 999.315(c) of the existing CCPA regulations until it can be replaced with new regulations for an optional opt-out preference signal that are consistent with the statute's requirements.

2. **The opt-out preference signal should require the consumer to indicate their state of residence and that information should be transmitted as part of the signal.** While California and Colorado are currently the only two states with opt-out preference signals enshrined into law, there are already substantive differences in the types of opt outs each state provides. Furthermore, other states are likely to follow suit with their own opt-out signals, which will inevitably create further divergence in compliance requirements.[15] Meanwhile, both the CPRA and ColoPA

[15] The VCDPA Work Group of the Joint Commission on Technology and Science recently issued its final report pursuant to the VCDPA, which included a recommendation to "[e]ncourage the development of third-party software and browser extensions to allow users to universally opt out of data collection, rather than individually from each website." Joint Commission on Technology and Science, Virginia Consumer Data Protection Act Work Group, 2021 Final Report, https://rga.lis.virginia.gov/Published/2021/RD595/PDF. The opt-out rights provided by the VCDPA are very similar to those provided by the ColoPA, but the VCDPA's definition of "sale" is substantively different from the ColoPA, CCPA, and CPRA as it includes only exchanges of personal data for monetary consideration.

require that consumers be informed about the opt-out choices available to them, which differ as explained above.

Nevertheless, opt-out preference signals are likely to be transmitted in circumstances where the business does not know the actual identity of the consumer, let alone the consumer's state of residence. It is thus important for platforms to be able to know the consumer's state of residence to present the correct opt-out choices and for businesses to know the same to apply the correct opt-out rights.[16]

3. **The Agency should work with the Colorado Attorney General to create an interoperable technical standard for opt-out preference signals.** Section 6-1-1313(2)(e) of the ColoPA requires the Colorado Attorney General, by July 1, 2023, to "[a]dopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the United States." Given that the CPRA regulations will most likely precede the ColoPA's regulations, it would be prudent for the Agency to work with the Colorado Attorney General to ensure that the technical requirements for the CPRA's opt-out preference signal do not inherently conflict with an opt-out preference signal that could be adopted under the ColoPA.

   In particular, by adopting our recommendation that the opt-out preference signal require the consumer to indicate their state of residence and to transmit that information as part of the signal, remaining parts of the signal could be used to indicate an opt-out preference specific to each state's requirements without having to transmit separate signals for each state. Additionally, allowing for a single header signal that is adaptable for each state's requirements will help avoid situations where a business receives multiple opt-out preference signals from a single consumer that potentially conflict with one another by consolidating the possible signals into a single value. For example, the signal might transmit the following values via a single header field to represent various opt-out preference scenarios under the CPRA or ColoPA:

---

[16] Requiring a consumer to provide their state of residence to be transmitted as part of the opt-out signal is consistent with the requirement in Section 1798.185(a)(19)(A)(ii) that the regulations "[e]nsure that opt-out preference signal . . . does not require that the consumer provide additional information beyond what is necessary" because, as explained above, knowing the consumer's state of residence is necessary to ensure that the business is able to apply the correct opt-out rights to the signal received. Furthermore, knowing the consumer's state of residence is also necessary to "[e]nsure that the opt-out preference signal [for California] does not conflict with other commonly used privacy settings or tools that consumers may employ," as required by Section 1798.185(a)(19)(A)(iv), such as opt-out preference signals employed for Colorado or other states.

	Limit Use of Sensitive Personal Information (CPRA) *or* Opt Out of Targeted Advertising (ColoPA)	**Do Not Sell/Share (CPRA) *or* Do Not Sell (ColoPA)**	**Opt Out of All**
CPRA	CA10	CA01	CA11
ColoPA	CO10	CO01	CO11

4. **Businesses should not be required to apply opt-out preference signals transmitted via one platform to any other platform where the business is not able to associate the signal with the consumer's activities on other platforms.** Section 1798.145(j)(3) of the CPRA states that a business is not required to "[m]aintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information" and Section 1798.145(j)(2) of the CPRA states that a business is not required to "[r]etain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained."

   Businesses will inevitably receive opt-out preference signals in circumstances where they do not know the actual identity of the consumer involved and the "sale" or "sharing" of the consumer's "personal information" is occurring solely with respect to identifiers tied to a single browser or device. When a business receives an opt-out preference signal (or indeed, any other opt-out request) in those circumstances (i.e., the business does not retain personal information necessary to link the consumer to other browsers or devices), the business should be permitted to honor that opt-out request within the confines of the personal information it possesses. Furthermore, the business should not be required to request additional personal information from the consumer to attempt to extend the consumer's opt-out request to other browsers or devices where that information is not necessary for the business's ordinary course of business.

5. **Businesses should be permitted to ignore or block an opt-out preference signal where the business is unable to accurately authenticate the consumer as a California resident or where the business has reasonable grounds to believe that the signal is fraudulent.** Section 1798.185(a)(19)(A)(i) requires that the regulations "[e]nsure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business." Fraud is an unfortunate reality that many advertisers and

publishers must constantly combat in the online advertising industry, with global losses estimated to run in the billions of dollars annually.[17]

Cybercriminals carry out this fraud by using bots to impersonate consumers, drive up ad impressions, and engage in other manipulative and dishonest behavior. It is therefore crucial that businesses be permitted to scan for and defend themselves against such fraudulent activity, including where such activity seeks to exploit opt-out preference signals (possibly to attempt to evade detection). Otherwise, ad fraud perpetrators or unscrupulous competitors, as manufacturers of such bots, would effectively be permitted to "unfairly disadvantage another business" through the sending of such signals.

Perhaps recognizing the crucial importance of fraud prevention, the ColoPA expressly requires that its rules for an opt-out preference signal "[p]ermit the controller to accurately authenticate the consumer as a resident of this state and determine that the mechanism represents a legitimate request to opt out . . . ."[18] The Agency should incorporate the same permission into the CPRA regulations.

8. ***Definitions and Categories***

8.e: Service providers and contractors should be permitted to combine data from different sources for security and integrity purposes.

Under the CPRA, businesses that make consumer personal information available to their contractors and service providers (together, "Service Providers") must contractually prohibit them from combining that personal information with personal information from other sources.[19] In our clients' experience, Service Providers that process consumer personal information for security and integrity purposes often need to combine personal information from multiple sources to provide effective security and fraud detection services. Combining personal data from multiple sources may, for example, enable a Service Provider to better identify and remediate malicious activity affecting multiple businesses. This activity is currently supported by Section 999.314(c)(4) of the existing CCPA regulations, which permits a service provider to retain, use, and disclose personal information obtained in the course of providing services "[t]o detect data security incidents or protect against fraudulent or illegal activity."

---

[17] *See* Farnaz M. Alemi, *How Cybercriminals Are Stealing Your Ad Dollars*, Bloomberg Law, May 27, 2021, https://news.bloomberglaw.com/securities-law/how-cybercriminals-are-stealing-your-ad-dollars.

[18] Colo. Rev Stat. § 6-1-1313(2)(f).

[19] Cal. Civ. Code § 1798.140(j)(1)(A)(iv), (ag)(1)(D).

Although "[h]elping to ensure security and integrity" is a business purpose already recognized in the CPRA,[20] it is unclear whether Service Providers may combine consumer personal information for such purposes. The CPRA explains that a Service Provider "may combine personal information to perform any business purposes as defined in regulations adopted pursuant to paragraph [1798.185(a)(10)]."[21] Section 1798.185(a)(10) in turn gives the Agency authority to adopt regulations that "further defin[e] the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources . . . ." As currently drafted, it is unclear whether the business purposes defined in Section 1798.140(e) are read into Section 1798.185(a)(10), or whether the Agency needs to expressly identify each business purpose for which a Service Provider may combine consumer personal information.

The Agency should clarify that Service Providers may combine consumer personal information for security and integrity purposes and carry forward the existing principle stated in Section 999.314(c)(4) of the CCPA regulations. Businesses and Service Providers would further benefit from clarity regarding whether Service Providers may combine consumer personal information in connection with the business purposes defined in Section 1798.140(e).

9. ***Additional Comments***

9: Service providers and contractors should be permitted to use consumer personal information for their own security and integrity purposes.

Section 1798.185(a)(11) of the CPRA directs the Agency to specify when service providers and contractors may use consumer personal information that was provided to them under a written contract with a business, for the service providers' or contractors' own business purposes. The Agency should adopt a regulation permitting service providers and contractors to use consumers' personal information for security and integrity purposes. This limited use would promote Section 1798.185(a)(11)'s "goal of maximizing consumer privacy," by enabling service providers and contractors to better protect consumer personal information.

9: Businesses should be able to comply with Section 1798.100(d) by requiring their service providers or contractors to include contractual terms with their downstream service providers and contractors.

Section 1798.100(d) of the CPRA requires a business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose to enter into an agreement with the third party, service provider, or contractor containing various terms. In practice, businesses commonly enter into agreements with service providers that manage various

[20] Cal. Civ. Code § 1798.140(e)(2).

[21] Cal. Civ. Code § 1798.140(j)(1)(A)(iv), (ag)(1)(D) (emphasis added).

subcontractors. A business may directly provide personal information to those subcontractors so that the service provider and its subcontractors can provide services to the business.

We request that the Agency clarify that the CPRA permits businesses to comply with Section 1798.100(d) by contractually requiring their service providers and contractors to flow down the required terms in their contracts with subcontractors rather than having to enter into agreements with each subcontractor. Requiring businesses to enter into agreements with each subcontractor, with whom the business often does not have a direct relationship, would be unreasonably burdensome, inconsistent with global privacy laws, and would provide no meaningful benefit to consumers.

Sincerely,

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

[redacted]

Tracy R. Shapiro

[redacted]

Eddie Holman

From: Evan Enzer [redacted]
Sent: 11/8/2021 6:43:04 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Jacqueline Singh [redacted]; Albert Fox Cahn [redacted]
Subject: Comments on preliminary rulemaking
Attachments: 2021-11-08 Invitation for preliminary comments on CPRA 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.

Good evening,

Please see S.T.O.P.'s attached comment on the CPPA's preliminary rulemaking.

Thank you for the opportunity to comment.

Best,

Evan Enzer

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

Evan Enzer
Legal Fellow
Pronouns: he/his/him
**Bar Admission Pending*

Surveillance Technology Oversight Project
40 Rector Street, 9th Floor
New York, NY 10006
[redacted]
www.StopSpying.org

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (646) 602-5600

COMMENT OF THE SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

TO THE CALIFORNIA PRIVACY PROTECTION AGENCY

IN RESPONSE TO INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING UNDER THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

PROCEEDING NO. 01-21

SUBMITTED NOVEMBER 8, 2021

Introduction

The Surveillance Technology Oversight Project ("S.T.O.P.") submits this comment in response to the California Privacy Protection Agency's ("CPPA") invitation for preliminary comments on the proposed rulemaking. S.T.O.P. is a community-centered privacy and civil rights organization that organizes for policy change at the state and local levels. We also work with law firms to protect Californians' rights under the California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA"). We are especially concerned about how government use of biometric identification technology entrenches historical biases. Consistent with this concern, we respectfully ask that the CPPA consider mitigating this problem by protecting consumers' biometric data.

S.T.O.P. suggests that the CPPA protects biometric information in several ways. The CPPA should:

- To the extent possible, require businesses to obtain opt-in consent before using or disclosing biometric data to ensure people are given an upfront choice as to whether their biometric data is used, and how.
- Require businesses to streamline the opt-out and deletion process, as any overly onerous process will unnecessarily burden consumers, especially when dealing with many companies.
- Require businesses that collect and use biometric data to implement comprehensive risk assessments that accurately represent the cybersecurity and privacy risks associated with the technologies that collect, store, and process biometric data.

Background

The CPRA recognizes that some categories of information are especially sensitive, including biometric data that identifies a consumer. Biometric identification technology is problematic because it is overly invasive, unreliable (as is often the case with marginalized populations like women, trans, non-binary, and BIPOC individuals), and chills free expression.[1] For these reasons, the CPPA should implement a system especially attuned to the outsized risks associated with biometric data.

Californians are worried about the government's extensive biometric surveillance network. As a result, cities in every region enacted ordinances regulating municipal procurement of surveillance technologies.[2] Some have gone further, banning facial recognition altogether.[3] However, law enforcement sidesteps public will by purchasing data on the open market.[4] The California Electronic Communications Privacy Act's warrant provision does not consistently apply to these

---

[1] Brendan F. Klare et. al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transaction on Info. Forensics and Sec., No 6, 1789, 1789 (2012), https://s3.documentcloud.org/documents/2850196/Face-Recognition-Performance-Role-of-Demographic.pdf.
[2] Ari Chivukula et. al., *Local Surveillance Oversight Ordinances* 1-3 (2021), https://www.law.berkeley.edu/wp-content/uploads/2021/02/Local-Surveillance-Ordinances-White-Paper.pdf.
[3] Jill Cowan, *San Francisco Banned Facial Recognition. Will California Follow?*, NY Times (July 1, 2019), https://www.nytimes.com/2019/07/01/us/facial-recognition-san-francisco.html.
[4] Elizabeth Goitein, *The Government can't Seize your Digital data. Except by Buying it*, Wash. Post, (April 26, 2021), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/.

procurements, leaving a massive gap in state law.[5] However, the CPPA could address this troubling practice by effectuating Californians' right to control their data through opt-out and deletion.

Recommendations

Consent-based consumer opt-in to the extent possible via CPRA

Adopt an opt-in methodology for biometric data

S.T.O.P. believes that corporations should end the destructive practice of collecting biometric data, but if they continue, opt-in consent is the bare minimum necessary to effectuate consumers' rights. Corporations' response to the first iteration of California's comprehensive privacy law demonstrates why an opt-in methodology is imperative. After the legislature enacted the CCPA, businesses implemented confusing and uncomfortably invasive procedures to incentivize consumers to forego their statutory rights."[6] The Attorney General addressed this problem in previous regulations, but many large corporations still implement a complicated opt-out. As the CRPA and CPPA place the burden on consumers to opt-out from every business collecting their data, these onerous deceptive practices effectively destroy any semblance of consent.

Also, while the CPRA requires a business to provide notice before collecting data, that notice is effectively meaningless in many situations. For example, in a mall storefront, it is unlikely consumers will notice signage informing them that the business uses facial recognition to identify them, especially if they have a disability, do not speak English, or are impacted by any other combination of factors. Therefore, an opt-in consent methodology is critical to effectuating consumers' right to control their biometric privacy without an undue burden.

Streamline the consumer opt-out and deletion process

Ultimately, streamlining the opt-out and deletion processes is a grossly inadequate plan for protecting California's privacy. Still, we understand that the statute may constrain the CPPA, and with that understanding, we encourage the agency to take every action reasonably under its control. If the CPPA concludes that it cannot do more, it should at least standardize and simplify the deletion and opt-out processes. However, this must only be an incremental step towards opt-in consent and a complete ban.

At the absolute minimum, in addition to requiring a business to honor the universal opt-out switch and other design specifications within the CPRA's text, any deletion or opt-out systems should include the following protections:

- Clear, prominent, and meaningful notice in both digital and physical environments, by both visual and auditory means, which will ensure accessibility for people experiencing disabilities or other circumstances which may impact the interpretation of such signage.

---

[5] Cal. Penal Code § 1546.1.

[6] Consumer Reports, Comment Letter on Third Set of Proposed Regulations Implementing the California Consumer Privacy Act (Oct 28, 2020), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-written-comm-3rd-15-day-period.pdf.

- A user-friendly mechanism. For the opt-out, this should require no more than two clicks. This should include clicking a clearly labeled button to open an easily understandable short form preferences window, then clicking a clearly labeled opt-out switch. For deletion, it should not require more clicks or additional information than necessary to carry out the request.

While it is not nearly enough, these changes would incrementally improve the opt-out and deletion processes.

Cybersecurity and privacy risk assessment requirements

Businesses must prevent threats from leaking data to the open web to minimize law enforcement's access to personal information. Law does not prevent law enforcement from aggregating and analyzing public data, so adequate cybersecurity is essential. Without it, insiders and outsiders alike would have ready access to troves of personal data they could disclose to anyone with internet access, including law enforcement. To mitigate that risk, we recommend the following industry-standard best practices. But, of course, we encourage the CPPA to look beyond them for even more stringent requirements.

Businesses that collect and use biometric information should implement comprehensive risk assessments that accurately represent cybersecurity and privacy risks associated with the technologies which collect, store, and process biometric data. These risk assessments should be conducted by an external, US-based, third-party auditing firm and should result in the production of a report summary in a specified format which should be accessible to the CPPA upon request. CPPA could compare this reporting to previous reports for indications of progress or lack thereof. This intentional transparency will create a strong incentive for businesses to continually improve their cybersecurity and privacy practices relating to information collection, storage, and processing.

At a minimum, the report summary should include a high-level overview of:

- The name of the third-party auditing firm.
- The specific systems in scope for the audit and a description of the methodology employed for the audit.
- Any critical- or high-risk privacy and cybersecurity vulnerabilities associated with any systems used to collect, store, and process personal information and sensitive personal information.
- Recommended actions provided by the third-party auditor, describing the course of action which a business should take to resolve any vulnerabilities.

As businesses are already bound to additional cybersecurity-related legal and regulatory compliance requirements, this provision will introduce additional transparency for the CPPA regarding a business's cybersecurity and privacy activities while minimizing the additional burden on businesses.

Thank you for the opportunity to comment on the preliminary rulemaking. We look forward to working with you to protect Californians and would be delighted to discuss biometric privacy further.

From: Hayley Tsukayama [redacted]
Sent: 11/8/2021 4:56:06 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: Re: Comments on PRO 01-21 from the Electronic Frontier Foundation, ACLU California Action and others
Attachments: 2021-10-20CPPACommentsEFFACLUCA.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,

Apologies for the resubmission, but this version has been corrected to reflect Common Sense Media's support of the section regarding "Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information." I apologize for the oversight; please use this version.

Hayley Tsukayama

From: Hayley Tsukayama <[redacted]>
Date: Monday, November 8, 2021 at 4:43 PM
To: regulations@cppa.ca.gov <regulations@cppa.ca.gov>
Cc: Becca Cramer-Mowder <[redacted]>
Subject: Comments on PRO 01-21 from the Electronic Frontier Foundation, ACLU California Action and others

Good afternoon,

My name is Hayley Tsukayama and I am submitting comments on behalf of the Electronic Frontier Foundation and the ACLU California Action in response to PRO 01-21. The full document represents the views of both of our organizations. I have also cc'd Becca Cramer-Mowder, Legislative Coordinator & Advocate at the ACLU California Action.

I would like to note that sections of these comments also have the support of the National Fair Housing Alliance and Common Sense Media. Each discussion section opens with a statement outlining who is in support of that section. If it would be more convenient, after the deadline has passed, for the Agency to receive these in separate files, please let me know.

As noted in the comments, if you would like to contact Common Sense Media, please direct your communications to Irene Ly, Policy Counsel ([redacted]); to contact the National Fair Housing Alliance, please direct your communications to Michael Akinwumi ([redacted]) Chief Tech Equity Officer or Snigdha Sharma, FAIR Ops Team Lead & Tech Equity Analyst ([redacted]) at the NHFA's Tech Equity Initiative.

Thank you for the opportunity to comment. Please do not hesitate to reach out with any questions.

Sincerely,
Hayley Tsukayama

--
Hayley Tsukayama

Legislative Activist
CIPP/US

Electronic Frontier Foundation | San Francisco, CA
https://www.eff.org/
Pronouns: she/her

BEFORE THE CALIFORNIA PRIVACY PROTECTION AGENCY
OF THE STATE OF CALIFORNIA

Proceeding No. 01-21

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION AND ACLU CALIFORNIA ACTION IN RESPONSE TO THE REQUEST FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING UNDER THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

November 8, 2021

I. INTRODUCTION

In accordance with Government Code sections 11346, subdivision (b), and 11346.45, EFF is writing in reply to the invitation issued by the California Privacy Protection Agency ("the Agency") seeking input from stakeholders in developing regulations as directed by the California Privacy Rights Act (CPRA), and the California Privacy Protection Act (CCPA) as modified by the CPRA.

ABOUT THE PARTIES

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 35,000 dues-paying members (with several thousand California members) and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. EFF has engaged in discussions around privacy regulations in California and throughout the country at the state and federal level. EFF has previously submitted comments to the California Attorney General regarding rulemaking for the California Consumer Privacy Act (CCPA), both as an individual organization and in collaboration with other leading privacy advocacy organizations.

ACLU California Action protects civil liberties and civil rights, advances equity, justice, and freedom, and dismantles systems rooted in oppression and discrimination. ACLU California Action has an abiding interest in the promotion of the guarantees of individual rights embodied in the federal and state constitutions, including the right to privacy guaranteed by the California Constitution and the right to due process. ACLU California Action is a 501(c)(4) organization associated with the three ACLU affiliates in California—ACLU of Northern California, ACLU of Southern California, and ACLU of San Diego and Imperial Counties.

Sections of these comments also have the support of the National Fair Housing Alliance and Common Sense Media. Each discussion opens with a statement outlining who is in support of that section. If you would like to contact Common Sense Media, please direct your communications to Irene Ly, Policy Counsel ([redacted]); to contact the National Fair Housing Alliance, please direct your communications to Michael Akinwumi ([redacted]) Chief Tech Equity Officer or Snigdha Sharma, FAIR

Ops Team Lead & Tech Equity Analyst ([redacted]) at the NHFA's Tech Equity Initiative.

II. DISCUSSION

1. Defining Automated Decisionmaking: *This section reflects the views of EFF, the ACLU California Action, Common Sense Media, and the National Fair Housing Alliance.*

While the CPRA grants the Agency broad authority to write regulations regarding the rights to opt-out and to access information that informs automated decisionmaking (ADS), it does not define the term and what activities it covers. There has been much debate in legislatures across the country over what systems constitute automated decisionmaking—making them subject to stricter regulations.

Any definition of ADS should not assume that automated systems are any less biased or more trustworthy than human judgment. As such, we encourage the Agency to look at definitions proposed by Rashida Robinson in a forthcoming paper for the Maryland Law Review regarding government use of automated decision systems.[1] Robinson's definitions, while constructed for a different context than the Agency is charged with, touch on several applications of these systems that should be included as part of meaningful regulation of automated decisionmaking system. This includes a serious consideration of the potential for discriminatory outcomes that arise from their use.

- **Comprehensive ADS Definition:** "Automated Decision System" is any tool, software, system, process, function, program, method, model, and/or formula designed with or using computation to automate, analyze, aid, augment, and/or replace government decisions, judgments, and/or policy implementation. Automated decision systems impact opportunities, access, liberties, safety, rights, needs, behavior, residence, and/or status by prediction, scoring, analyzing, classifying, demarcating, recommending, allocating, listing, ranking, tracking, mapping,

[1] Richardson, Rashida, Defining and Demystifying Automated Decision Systems (March 24, 2021). Maryland Law Review, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3811708

optimizing, imputing, inferring, labeling, identifying, clustering, excluding, simulating, modeling, assessing, merging, processing, aggregating, and/or calculating.

- **Narrow ADS Definition:** "Automated Decision Systems" are any systems, software, or process that use computation to aid or replace government decisions, judgments, and/or policy implementation that impact opportunities, access, liberties, rights, and/or safety. Automated Decisions Systems can involve predicting, classifying, optimizing, identifying, and/or recommending.

2. Skepticism of "trade secrets" or "proprietary information" exemptions

We do not believe that the CPRA requires a trade secret exception for automated decisionmaking systems. There is a trade secrets exemption in the CPRA, but only for verified consumer requests. As such, if, for example, companies had to disclose information about ADS use publicly or to an agency, no verified consumer request would be required.

We encourage the Agency to resist any carveouts that allow businesses to hold back information by claiming trade secrets, proprietary information, or that the information is subject to non-disclosure agreements between parties and therefore cannot be shared with consumers—or in some cases, at a minimum with auditors and regulators.

One goal of automated decisionmaking regulation should be to improve understanding for the people directly affected by the decisions that are made. But it's not enough to think merely about the individual consumer—there is a collective, societal interest in understanding how companies are making important decisions about people, and in ensuring fairness in those decisions, given the well-documented discrimination that grows in algorithmic darkness. Companies should not be allowed to escape scrutiny by claiming the commercial need to protect their intellectual property or company information. Europe's General Data Protection Regulation (GDPR) says that in cases of automated decision-making, the data subject has the right to access "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[2] A right to an explanation—both why an

[2] *Art. 22 GDPR – automated individual decision-making, including profiling*. General Data Protection Regulation (GDPR). (2018, July 26). Retrieved October 30, 2021, from https://gdpr-info.eu/art-22-gdpr/.

entity is collecting information, and also how the system reached a final decision—is crucial to protecting consumers and should not be sacrificed by a trade secrets claim.

We have seen these kinds of assertions repeatedly in the criminal context, where companies have asserted that they cannot share information about how they have arrived at their conclusions in order to protect trade secrets, thus depriving individuals of information to understand how a company's algorithm was able to deprive them of their liberty[3].

In the consumer context, however, companies use automated decisionmaking systems to make significant decisions that have serious consequences for people's daily lives—such as who is approved for a mortgage[4], who is approved for a credit card[5], or who can receive a loan. Companies have shown they are not likely to disclose the inner workings of such systems on their own, preferring opacity—sometimes to hide the ways they have ignored problems with algorithms. To point to a particularly timely example, the recent Facebook whistleblower revelations indicate a very important fact: the major users of algorithmic processing in consumer-oriented businesses know, in great detail, what their products do. The type of information that we've seen from "the Facebook papers" clearly was considered by Facebook in making decisions about its algorithms, and clearly documented Facebook's evidence-based beliefs about how, for example, Instagram hurt female teenagers.[6] Yet the company has still refused to explain—to Congress, to its 2 billion users, or publicly—how, if at all, it responded to that information even in the face of clear threat of harm to some of its youngest users. These businesses know both what they are doing, and why, and they certainly know much more than the ordinary consumer. And, from the reactions of lawmakers in DC, the companies know much more than government regulators. Regulations from the CPPA have a chance to change that.

---

[3] Electronic Frontier Foundation. (2017, September 14). *EFF asks court: Can prosecutors hide behind trade secret privilege to convict you?* Electronic Frontier Foundation. Retrieved October 29, 2021, from https://www.eff.org/press/releases/eff-asks-court-can-prosecutors-hide-behind-trade-secret-privilege-convict-you.

[4] Martinez, E., & Kirchner, L. (2021, August 25). *The secret bias hidden in mortgage-approval algorithms – the Markup*. – The Markup. Retrieved October 29, 2021, from https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

[5] Vigdor, N. (2019, November 10). *Apple card investigated after gender discrimination complaints*. The New York Times. Retrieved October 29, 2021, from https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html.

[6] Olivia Solon, & David Ingram. (2021, October 25). The facebook papers: Documents reveal internal fury and dissent over site's policies. CNBC. Retrieved November 9, 2021, from https://www.cnbc.com/2021/10/25/the-facebook-papers-documents-reveal-internal-fury-and-dissent-over-sites-policies.html.

As the CPRA's text recognizes, it is critical to be able to evaluate the reasoning behind such decisions, to ensure there is no incorrect information and that automated decisionmaking systems are not simply repeating (or even amplifying) historic biases from the systems they seek to replace.

In response to an Agency access request, there should be no place for businesses to hide behind a trade secrets claim. In response to consumer requests, businesses should still be prepared to answer some simple questions, such as what factors were used in the decision, how those factors were weighted to reach that decision, and the confidence with which the system made that decision. Applied to a particular circumstance, a consumer may reasonably want to know why a particular ad—for a mental health app, for example, or for financial counseling—has been shown to them and what it may say about what's included in an advertising profile about them. They should have that right. Or, for example, in a case where a company finds that a consumer has perpetuated a fraud, the CPRA should allow the individual to receive information on how a company came to its conclusion about their behavior.

Without such information, the regulations do not fullfil the CPRA's promise to "include meaningful information about the logic involved in such decision- making processes, as well as a description of the likely outcome of the process with respect to the consumer.".

3. Profiling and Automated Decisionmaking

It is also important to consider the relationship between automated decisionmaking and profiling. Not all automated decisionmaking is profiling (and not all profiling involves ADS), but the two overlap significantly. To pull an example from the European Union's Article 29 working group[7]:

> Imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision-making process that does not necessarily involve profiling. It would, however, become a decision based on profiling if the driving habits of the individual were monitored over time, and, for example, the amount of fine imposed is the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations.

[7] Article 29 Data Protection Working Party. (2017, October 3). Article 29 Data Protection Working Party - European Commission. Retrieved October 30, 2021, from https://ec.europa.eu/newsroom/document.cfm?doc_id=47742.

In cases where the data that feeds a profile is determined through automated decisionmaking, consumers should be able to obtain information that allows them to understand how those decisions were made.

4. Automated Decisionmaking in the Workplace

It is also worth noting that the question of access and opt-out rights regarding automated decisionmaking systems and profiling takes on additional dimensions when considered in a workplace context. Employees are carved out many of the CPRA's protections at the moment, but that provision will sunset in 2023.

There is no question that workers face potentially grave consequences from unchecked use of automated decisionmaking systems. Electronic monitoring and data collection are used to inform systems in workplaces such as warehouses, to determine how quickly workers are completing their tasks, and how much time they spend on non-work tasks such as leaving the line to use the restroom.[8] Furthermore, companies such as Amazon have automated processes such as measuring "productivity" and even termination—decisions that can be made without input from a worker's supervisor.[9] Even in cases where a supervisor or other person can have input in a decision, interviews with Amazon employees reveal that the recommendation of these algorithms often remain unchanged even when presented with information explaining, for example, that an employee was not working for a valid reason—whether that's a bathroom break or a medical emergency such as a seizure.[10]

In an at-will employment context, the freely given consent of the individual can be difficult to obtain, because individuals are at a serious disadvantage in a situation where opting-out of automated decisionmaking, or asking to opt out of data sale or sharing, may cost them their job. Workers should have the right to negotiate through unions their right to the access of

[8] Evans, W. (2021, July 22). *Prime labor: Dangerous injuries at Amazon warehouses*. Reveal. Retrieved October 30, 2021, from https://revealnews.org/article/behind-the-smiles/.
[9] Lecher, C. (2019, April 25). *How Amazon automatically tracks and fires warehouse workers for 'productivity'*. The Verge. Retrieved October 31, 2021, from https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations?mod=article_inline.
[10] Liao, S. (2018, April 16). *Amazon warehouse workers skip bathroom breaks to keep their jobs, says report*. The Verge. Retrieved October 31, 2021, from https://www.theverge.com/2018/4/16/17243026/amazon-warehouse-jobs-worker-conditions-bathroom-breaks.

information, including those that feed into automated decisionmaking systems, as they apply to crucial decisions about their hiring, firing, discipline, promotion and daily working conditions. In non-unionized workplaces, workers should still be able to request and obtain information about data-driven decisions that materially affect their working conditions or employment. Workplaces should also be required to disclose the systems they use to workers, so that workers will have awareness of their rights in the first place.

Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information:
This section reflects the views of EFF, ACLU California Action, and Common Sense Media.

We believe that a vast amount of personal information becomes sensitive depending on the contexts, and therefore, we advocate that a separate category of "sensitive personal information" does not serve consumers well. We are also concerned that data that isn't within the "sensitive" category can be a proxy for data that is. A home address, for instance, can provide information about one's race. However, given that this is a newly created category under the CPRA, we do have concerns about highly sensitive types of information that are left out. These include but are not limited to:

- **immigration status** – disclosing or using a person's immigration status could cause serious repercussions for an individual, including discrimination based on that status.
- **connections among family members** – a data broker may use metadata to determine that two people belong to the same family or to the same household. This could, for example, allow for someone's address to be disclosed without their permission if another member of their household has a reason to disclose an address.
- **biometric information collected for a purpose other than identification –** biometric information is sensitive, particularly as it is both permanent and immutable. It should be protected even when it is not being used for identification purposes. A business might later change course and use that same biometric information to establish an individual's identity, at which point the law would apply— but the unregulated processing would already have occurred.

A better definition of sensitive personal information would include not only the information explicitly listed as sensitive in the CPRA and that we have listed in these comments, but also information from which any sensitive personal information could be inferred.

Furthermore, no disclosure of a consumer's sensitive personal information by a business should be permissible if the consumer has not given their consent. To do so would directly contradict the purpose of CPRA's consumer privacy rights.

We also strongly believe that all information—but especially sensitive personal information, if such a category must exist—should be shared on an opt-in basis in most cases, rather than on an opt-out basis.

Definitions and Categories

We appreciate the opportunity to offer feedback on change that could be made to the current definitions that underpin the California Consumer Privacy Act.

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

Please see our above comments on sensitive personal information.

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

This section reflects the views of EFF, ACLU California Action, and Common Sense Media.

Currently, "deidentified" information is defined as any information that cannot be linked to a particular consumer. This is at odds with the rest of the statute, which defines "personal information" as information that is linked or linkable to a consumer, household,[11] or consumer's device.[12] As "deidentified" data is considered not to be "personal information," we are concerned that the current definition of "deidentified" could be interpreted to carve out all personal information which is associated only with a household or consumer's device. We also believe it's prudent to clarify that anything which is considered a "probabilistic identifier" or "precise geolocation information" cannot be considered "deidentified."

[11] See CPRA section 140(v)(1)
[12] See CPRA section 140(x)

Therefore, we propose the following updates to the definition of "deidentified:"

(1) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, *consumer's device, or household*, provided that the business that possesses the information:

...

(2) *"Deidentified" does not include any information associated with a probabilistic identifier, or any set of information that can be used to create a probabilistic identifier. "Deidentified" does not include precise geolocation information.*

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

This section reflects the view of EFF and ACLU California Action.

The definition of "precise geolocation" currently in the CCPA, as amended by the CPRA, is insufficient. The distance described is too prescriptive and not applicable to all contexts. In urban areas, it may be too expansive to be useful; in rural areas, it may not be expansive enough.

EFF suggests that this definition should be expanded to cover instances where a business has several different measurements of location pertaining to a single device or individual, even in the absence of other personal information or identifiers. Geolocation information can be extremely sensitive, and it is often trivial to reidentify a set of location measurements. One famous study found that four spatiotemporal points, derived from credit card metadata, was enough to uniquely identify 90% of individuals from a set of 1.1 million people. Anecdotally, a dataset which includes the location of a person's home, their work, and where they spend Thanksgiving may be easy to reidentify, even if the location measurements are "coarse." And as the Supreme Court has affirmed, even coarse records of individual movements, such as those generated by cellular sites, are deserving of special legal protection. Any series of location data measurements associated with a single individual, device, or household should be considered "personal information" under CPRA.

We encourage the Agency to look at the definition of "non-precise geolocation information" in Sen. Edward Markey's bill, the "Algorithmic Justice and Online Platform Transparency Act" as a guide to aid in defining what is not considered precise geolocation information. While we do not agree with every part of this definition—for example, ZIP code

can be fairly precise in certain situations—the approach of defining what is not precise may prove more instructive than defining what is.

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

This section reflects the views of EFF and ACLU California Action.

We support the proposed regulations from the California Department of Justice (DOJ) to protect against what are commonly called "dark patterns" in their proposal published October 12, 2020—specifically at Section 999.315(h), within the third set of proposed modifications of CCPA regulations, which the California DOJ published on October 12.

Additional Comments:

This section reflects the views of EFF and ACLU California Action.

We believe that privacy law in California falls short of the mark of consumer protection, and have supported several bills to further privacy protections in this state, including Asm. Buffy Wicks' 2019 "Privacy for All" bill, AB 1760 — a bill we supported as a strong privacy bill that would remedy the CCPA's shortcomings.[13]

Key pieces of the bill that remain to be enacted in this state include, but are limited to:

-A private right of action, which ensures that every person can go to court to hold companies accountable when they violate the law and refuse to respect our rights.

- A full right to know, which includes not only who companies have shared information with, but also what information has been shared. When it comes to protecting our own privacy, consumers are at a huge disadvantage. Companies know what they collect, how they use it, and who they share it with. Consumers usually do not.

- Opt-in consent for all information sharing and selling, which would give consumers needed control over the ways personal information is shared in the modern digital world, including in ways people may not expect. That returns privacy power to the people.

We offer these suggestions not only as an indication of how far we believe California must still go to offer consumers meaningful ways to protect themselves from unwarranted or

[13] Wicks, B. (2019, April 4). *Bill text.* Bill Text - AB-1760 California Consumer Privacy Act of 2018. Retrieved November 8, 2021, from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1760.

unwanted data collection, but also as encouragement for the California Privacy Protection Agency to be bold in executing the goal—protection of privacy—outlined in its very name.

The Agency has been given broad latitude to shape privacy protections in this state; we encourage you to do so to the fullest of your abilities.

Dated: November 8, 2021

Respectfully submitted,

/s/ Hayley Tsukayama
Hayley Tsukayama
Legislative Activist
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Tel: [redacted]

Becca Cramer-Mowder
Legislative Coordinator & Advocate
ACLU California Action
1127 11th Street, Suite 501,
Sacramento, CA 95824
Tel: [redacted]

From: Garner, Sheree [redacted]
Sent: 11/8/2021 7:41:38 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Sahli, David [redacted]; Young, Liz [redacted]; Janis, David [redacted]; Garner, Sheree [redacted]
Subject: PRO 01-21 - Rocket Mortgage's Preliminary Comments on the Proposed Rulemaking Under the CPRA of 2020
Attachments: RM CPRA Preliminary Comments on Proposed Rulemaking.pdf

[EXTERNAL]: [redacted]

To Whom It May Concern:

On behalf of Rocket Mortgage, attached are our Preliminary Comments on the Proposed Rulemaking Under the California Privacy Rights Act of 2020.

Please feel free to contact me should there be any issues with opening and/or accessing the attached document.

Sincerely,

Sheree Garner

Sheree Garner | Regulatory Counsel – Government Affairs
Rocket Mortgage | [redacted]
LEGAL TEAM

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

California Privacy Protection Agency (CPPA)
ATTN: Ms. Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

RE: PRO 01-21: Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020

November 8, 2021

Dear Ms. Castanon:

Rocket Mortgage appreciates the opportunity to provide our response to the California Privacy Protection Agency's (hereinafter "CPPA" or "Agency") Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020. We commend the CPPA for its proactive stakeholder engagement in developing new regulations to determine whether changes to existing regulations are necessary and achieving the law's regulatory objectives in the most effective manner.

Detroit-based Rocket Mortgage, the nation's largest home mortgage lender, enables the American Dream of homeownership and financial freedom through its obsession with an industry-leading, digital-driven client experience. Rocket Mortgage closed $320 billion dollars of mortgage volume across all 50 states in 2020. In late 2015, it introduced the first fully digital, completely online mortgage experience. Currently, 99% of all home loans originated by the company utilize Rocket Mortgage technology. Rocket Mortgage moved its headquarters to downtown Detroit in 2010.

Today, Rocket Mortgage and Rocket Companies employ 24,000 full-time team members nationwide. The company generates loan production from web centers located in Detroit, Cleveland, and Phoenix and operates a centralized loan processing facility in Detroit. Rocket Mortgage ranked highest in the country for customer satisfaction for primary mortgage origination by J.D. Power for the past 11 consecutive years, 2010 – 2020, and ranked highest in the country for customer satisfaction among all mortgage servicers the past eight straight years, 2014 – 2021. Rocket Companies, Rocket Mortgage's parent company, ranked #5 on Fortune's list of the "100 Best Companies to Work For" in 2021 and has placed in the top third of the list for 18 consecutive years.

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

Rocket Mortgage's preliminary comments are as follows:

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

The CPRA directs the Agency to issue regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to 1) perform annual cybersecurity audits; and 2) submit to the Agency regular risk assessments regarding their processing of personal information.

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

Rocket Mortgage Feedback:

- There must be a clear standard and threshold for what processing of personal information presents a significant risk to consumer privacy and security.
- The criteria for which the standard is comprised should be based on objective criteria.
- The standard must outline whether the risk is based on the inherent risk or takes outlined controls into consideration.

Subtopic: 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"?

Rocket Mortgage Feedback:

- These audits should be sufficiently broad to give businesses leeway to meet the requirements of the audit while also performing audits for compliance with federal and other state cybersecurity laws.
- There must be a clearly defined procedure for when and how the state may request findings of the audit. No delivery of audit findings should be authorized outside of a regulatory examination, investigation, inquiry, or request by the authorized governing body for the state of California.
- No details of an audit summary should be made public as it compromises trade secrets, proprietary information, or cybersecurity vulnerabilities to wrongdoers.

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

- Given the sensitivity of the data in these audits, all audits should happen onsite to ensure sensitive information (client, employee, etc.) is not leaving the company's secured environment.

Subtopic: 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?

Rocket Mortgage Feedback:

- The State of California should comprehensively outline the requirements for the performance of the risk assessment, including (but not limited to):
  - Procedures for performing a risk assessment
  - The contents of the results/findings of the risk assessment
  - Formatting and submission requirements

Subtopic: 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.

Rocket Mortgage Feedback:

- Trade secrets are not defined and will need to be. Trade secrets are likely material in calculating the weight of a business's interest in the processing of personal information, but the definition provides that "nothing in this section shall require a business to divulge trade secrets". Companies will spend a large amount of time and money defending what information is protected as a trade secret without this definition.

TOPIC: Automated Decision-making

The CPRA provides for regulations governing consumers' "access and opt-out rights with respect to businesses' use of automated decision-making technology."

Subtopic: What activities should be deemed to constitute "automated decision-making technology" and/or "profiling"?

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

Rocket Mortgage Feedback:

- Automated decision-making technology should be specifically defined to decisions that produce legal or similarly significant effects.
- Many industries like the mortgage industry are governed by other anti-discrimination laws to prevent profiling and similar problematics uses of automated decision making and should have exemptions in place for transactional automated decision making, including marketing and promotional efforts.
- Automated decision-making is key to removing subjective decision-making by individuals that are vulnerable to conscious and unconscious biases. The intended outcome of the regulation can be achieved by performance of regression testing during examinations by state regulatory bodies.
- The regulation must make it clear that a company is not discriminating if it cannot offer products or services if a consumer opts out of the use of automated decision-making technology.

Subtopic: 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.

Rocket Mortgage Feedback:

- The current language provides no safe harbor or protection of trade secrets and needs to include that as a company protection. Right to know requests may be used to reverse engineer intellectual property with overburdensome requirements in this space.
- It is more appropriate to regulate what information cannot be used rather than require companies to divulge criteria and categories of information used in trade secrets.

Subtopic: What information businesses must provide to consumers in response to access requests, including what businesses must do to provide "meaningful information about the logic" involved in the automated decision-making process.

Rocket Mortgage Feedback:

- Meaningful information to a consumer about the logic is unduly burdensome to require a company to track, personalize, and provide.
- Companies should be required to provide information in their privacy notice that outlines what types of data are used in AI/ML models at the company, but nothing beyond what is publicly available and does not pose undue risk to the company to provide.

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

- A key reason companies used AI/ML and data modeling is to make decisions on buckets of largely depersonalized data that will advise on specific trends. Putting in the tracking mechanisms to provide this information to a consumer puts them significantly at more risk because the models would have to account for a store unique sensitive information that it may not need otherwise just to get the information to the consumer.

Subtopic: 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.

Rocket Mortgage Feedback:

- Companies should not be penalized for not providing products or services to individuals exercising this opt-out right.
- It would be insufficient to create an exception for automated decision necessary for the delivery of a product or service, as "necessary" is a factual question and would create the onerous task for business to dispute whether a product or service could be offered or performed without the use of automated technology intrinsic to a company's day-to-day operation.

TOPIC: Audits Performed by the Agency

The CPRA gives the Agency the authority to audit businesses' compliance with the law.

Subtopic: What should be the scope of the Agency's audit authority?

Rocket Mortgage Feedback:

- Audit capabilities should be based solely on the CCPA and CPRA regulations, and should not take into account additional civil codes or other legislation unless adopted or referenced directly within the CCPA CPRA, or any additional privacy legislation.
- The authority to conduct an audit should be triggered by threshold criteria such as a consumer complaint.
- The threshold criteria must be objective and equitable across all industries so that the Agency isn't given unfettered authority to target certain companies based on size and/or profitability.

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

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

Rocket Mortgage Feedback:

- The Agency should either use an objective threshold or mirror the CFPB consumer complaint process.

Subtopic: The safeguards the Agency should adopt to protect consumers' personal information from disclosure to an audit.

Rocket Mortgage Feedback:

- All audit requests should be performed onsite if any personal information is exposed on any client, and companies should not be required to produce unmasked documentation to auditors.
- Any documentation provided should be delivered via secured portal as opposed to email.
- Any findings and results should not be made public so the company does not expose cybersecurity weaknesses to potential malicious actors.

TOPIC: Consumers' Right to Delete, Right to Correct, and Right to Know

The CCPA gives consumers certain rights to manage their personal information held by businesses, including the right to request deletion of personal information; the right to know what personal information is being collected; the right to access that personal information; and the right to know what categories of personal information are being sold or shared, and to whom.19 The CPRA amended the CCPA to add a new right: the right to request correction of inaccurate personal information.

The Attorney General has adopted regulations providing rules and procedures to facilitate the right to know and the right to delete. The CPRA additionally provides for regulations that establish rules and procedures to facilitate the new right to correct.

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

Rocket Mortgage Feedback:

- Any right to correct, must correct information that was/is inaccurate based on point in time. If a transaction was performed under a name and that person later changes the name, the records moving forward may be updated to reflect the name change but there

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

should be no obligation to update the historical documents as the information is not inaccurate.

- Any company with existing correction procedures in place should be allowed to substitute the formalized VCR process for right to correct with their existing process, given that their process is reasonably compliant.

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

Rocket Mortgage Feedback:

- Businesses that already have correction processes in place should not be required to comply with this additional right. Companies should be required to maintain a policy around correction of data, especially as it relates to data integrity, confidentiality, and availability, but nothing further.
- Companies should be allowed to refuse this right to consumers who utilize the right to overzealously correct data, attempt to use the right to commit fraud, etc.

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

Rocket Mortgage Feedback:

- All requirements must mimic the right to know, access, and delete.

Subtopic: 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

Rocket Mortgage Feedback:

- All unstructured data should be exempt.
- All data that does not materially alter the consumer's experience with the company should be exempt.
- Companies should not be penalized for not correcting data unless the consumer can prove that they had an adverse impact or experience as a result of the incorrect data.
- All existing correction processes should be considered valid in lieu of a formal VCR.

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

Subtopic: 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.

Rocket Mortgage Feedback:

- Consumers should be allowed to provide a written addendum, but ultimately the business should make the call on whether the information is correctable. Allowing clients to materially alter their own files could result in clients attempting to commit fraud by altering data that most companies do not have control over --for example, credit data/eligibility/worthiness.
- The business should store the written addendum and should be allowed to provide a template to consumers to fill out (ex. fill out this form, we'll correct your data if you can). Instead of providing an actual addendum, the request itself should fulfill any auditing that needs to occur without the additional documentation.
- It is important that companies with a GLBA exception are able to exercise that exception in this space.

TOPIC: 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

The CCPA gives consumers the right to opt out of the sale of their personal information by covered businesses. In 2020, the Attorney General adopted regulations to implement consumers' right to opt out of the selling of their personal data under the CCPA. The CPRA now provides for additional rulemaking to update the CCPA rules on the right to opt-out of the sale of personal information, and to create rules to limit the use of sensitive personal information, and to account for other amendments.

Subtopic: 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?

Rocket Mortgage Feedback:

- There must be a standardized and universally approved signal to prevent the over burdensome mandate that business systems be able to receive and ingest signals from every system, technology, or platform sending unique signals. This will bring greater cross-industry continuity in delivery of these services and expediency and efficiency to comply with such requests.

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

Subtopic: 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.

Rocket Mortgage Feedback:

- Rocket Mortgage offers no commentary on opt out preferences for anyone under the age of 18. We comply with COPPA and take all reasonable measures to block usage of our digital experiences, products, and services, along with collection of data from individuals who do not qualify for a mortgage due to age.

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

Rocket Mortgage Feedback:

- This should be consistent with process and timing requirements for other CCPA allotted rights.

Subtopic: 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.

Rocket Mortgage Feedback:

- Businesses should have no obligation to re-prompt clients in a pre-scripted way. The client should be directed on how to change their opt in/out preference via the privacy policy. Prescribing a way that the design of this opt in/out experience exists outside of having one centralized resource for information will not be scalable for companies that have to comply state by state with privacy legislation.

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

The CCPA gives businesses certain responsibilities, and consumers certain rights, related to consumers' personal information. The CPRA amends the CCPA to give consumers additional rights over a new category of information: "sensitive personal information," and directs the Agency to amend existing regulations and/or issue new regulations to implement these

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

rights. These rights include the new right to limit the use and disclosure of sensitive personal information discussed above.

Subtopic: 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?

Rocket Mortgage Feedback:

- Sensitive personal information should be better defined to include personal characteristics (protected classes), and the most sensitive of personal information. Usage should be exempted if it's required for transaction (ex. Only for marketing usage)

Subtopic: 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?

Rocket Mortgage Feedback:

- Permissible use and disclosure should not be heavily regulated but should be readily available and apparent to the consumer via the privacy policy. Mandating prescriptive solutions in this area will cause unnecessary grief for consumers working with companies that are not in the industry that the CPRA/CCPA are most looking to reform (ex. financial institutions and potential conflicts with other laws. All other law should take precedence to the CPRA/CCPA).

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

When businesses are required to disclose specific pieces of information to a consumer, the CPRA generally requires the disclosure to cover the 12 months prior to a consumer's request. However, for all information processed on, or after January 1, 2022, consumers may request, and businesses must disclose, information beyond the 12-month window subject to the exception described in a) below.

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

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

Rocket Mortgage Feedback:

- Any lookback period should not exceed any federally mandated minimum retention periods.

TOPIC: 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.

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

Rocket Mortgage Feedback:

- All definitions should align with definitions from other states and/or the GDPR.

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

Rocket Mortgage Feedback:

- All definitions should align with definitions from other states and/or the GDPR.

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

Rocket Mortgage Feedback:

- Unique identifiers should be considered de-identified provided the information it is associated with cannot be combined to identify an individual.

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

Rocket Mortgage Feedback:

- Designated methods for submission of requests should take into account the fact that an acceptable alternative may be existing business processes.

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

ROCKET Mortgage

1050 Woodward Ave.
Detroit, MI 48226

Rocket Mortgage Feedback:

- The definition should be broad enough to not unintentionally limit business's ability to have unique, yet user friendly experiences.

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

Rocket Mortgage Feedback:

- Precise geolocation should be exempted from sensitive data if it is only used for providing the product or services requested by the consumer.

Subtopic: What definition of "specific pieces of information obtained from the consumer" the Agency should adopt?

Rocket Mortgage Feedback:

- The definition should specify "specific pieces of information obtained from the consumer" does not include company trade secrets or compliance controls. It should only include specific pieces of information provided or authorized by the consumer for the business to receive such information. Businesses should be permitted to produce summaries of the specific pieces of information held. This will provide sufficient information for the consumer to exercise a right on such information but 1) avoid over burdensome productions of information and 2) protects consumer from fraudsters by avoiding granularity of sensitive data points. Businesses should not be required to produce duplicative specific pieces of information. This will avoid over burdensome productions, such as work logs, while still informing the proper categories of information.

Rocket Mortgage looks forward to the opportunity to provide additional comments when the Agency proceeds with its notice of proposed rulemaking action on the final CPRA regulations. In the meantime, should you have any questions or need addition input from us, please feel free to contact David Sahli at [redacted].

Sincerely,

[redacted]

David R. Janis
Associate General Counsel, Rocket Mortgage

From: Snell, James (Jim) (Perkins Coie) [redacted]
Sent: 11/8/2021 8:10:28 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: 2021-11-08 Letter to CPPA.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 attached a client's CPRA comments. We appreciate the opportunity the Agency has provided for comments.
Best,

James (Jim) Snell | **Perkins Coie LLP**
PARTNER
3150 Porter Drive
Palo Alto, CA 94304-1212
[redacted]
F. +1.650.838.4567
[redacted]

PERKINSCOIE

3150 Porter Drive
Palo Alto, CA 94304-1212

+1.650.838.4300
+1.650.838.4350
PerkinsCoie.com

November 8, 2021

James G. Snell
[redacted]
F. +1.650.838.4567

VIA EMAIL

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

To Whom It May Concern:

Please find below comments on behalf of a client with respect to the September 22, 2021 Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act ("CPRA") of 2020. To be clear, these comments are not provided on behalf of Perkins Coie LLP, and do not necessarily reflect the views of Perkins Coie LLP, but instead reflect comments from a client who asked that we submit such comments on their behalf. We thank the California Privacy Protection Agency ("Agency") and staff for considering these comments and for providing businesses with needed clarity on the law.

1. Guiding Principles for Meeting the CPRA's Regulatory Objectives:

Our client thanks the Agency for its efforts to provide businesses with needed clarity with respect to CPRA compliance. As the Agency considers input from stakeholders in achieving the law's regulatory objectives, we offer the following guiding principles for the Agency to consider as it moves forward in the rulemaking process:

(1) The Agency Should Align Regulations With Other Similar Privacy Laws To Promote Privacy-Preserving Business Practices And Consumer Understanding.

The CPRA acknowledges that, "[t]o the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions."[1] In addition, one of the Agency's functions under the law is to "[c]ooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections."[2] The Regulations should thus align with other similar privacy laws that advance the same policy goals

[1] CPRA Sec. 2, Findings and Declarations.
[2] California Civil Code, § 1798.199.40.(i)

as the CPRA. This would best promote privacy-preserving business practices and consumer understanding.

For example, both Colorado and Virginia have passed their own comprehensive consumer privacy laws since the CPRA passed; each of which will also take effect in 2023 and will impose business obligations that are substantively similar to those under the CPRA. Such obligations include: (1) providing notice of privacy practices; (2) providing consumer rights to access, delete, and correct their information; and (3) allowing consumers to opt out of the use of their information for targeted advertising purposes. The Agency should ensure that CPRA compliance obligations are consistent with these and other privacy laws. Consistency will enhance understanding and protections for personal information, while divergence would create confusion, unnecessary expense, and put personal information at risk. We therefore urge the Agency to enable businesses to meet their compliance obligations across jurisdictions via similar mechanisms and processes, leading to clear, streamlined policies, and ultimately helping consumers understand how their information is being used, and for what purposes.

One example of how to align regulations with other similar privacy laws is to give businesses flexibility in how they design notices of opt out rights. Such flexibility would allow companies to frame such notices in a context and format that makes sense to users based on the company's particular products and services, and where those products and services are offered. Specifically, we recommend that the Agency clarify that the CPRA permits businesses to utilize a single, clearly-labeled link on their homepage rather than multiple links to certain specified consumer rights, assuming, of course, that such a link is clear and allows consumers to exercise the choices available to them under the law.[3] Providing clarity on this matter would encourage companies to build unified compliance programs that align with similar laws in other jurisdictions to the benefit of all consumers. Such flexibility is both more practical and serves to further the policy goals of the CPRA more so than highly prescriptive programs that would confuse consumers and be inconsistent with similar language used to meet opt out obligations under similar laws.

(2) The Agency Should Allow Businesses Flexibility in Meeting Their Compliance Obligations Under the Law.

We urge the Agency to promote flexibility in the ways in which businesses may meet their compliance obligations under the CPRA. For example, in enabling consumers to submit rights requests to a business, the Agency should refrain from adopting highly prescriptive obligations that may complicate compliance obligations or lead to consumer confusion. Rather,

[3] California Civil Code, § 1798.135(a)(3) ("[a] business may utilize a single, clearly-labeled link on the business's internet homepage(s), in lieu of complying with" the precise wording and hosting of two separate links, "if such link easily allows a consumer to opt-out of the sale or sharing of the consumer's personal Information and to limit the use or disclosure of the consumer's sensitive personal information").

the Agency should embrace the law's mandate that "[c]onsumers or their authorized agents should be able to exercise these options through easily accessible self-serve tools."[4] Thus, we urge the Agency to acknowledge and accept the self-serve tools and other mechanisms that many companies already have in place to give consumers tools to exercise choice with respect to their information.

The Agency can also embrace flexibility with respect to responding to consumer requests to correct information held about them. The CPRA provides that the Agency should design this standard "taking into account available technology, security concerns, and the burden on the business." Practically, then, the obligation on a business should extend to information that a consumer has provided *directly* to the business, but not to information observed about a consumer's use of the business's services to the extent reasonable, and a business should not, for instance, be obligated to correct highly technical or unstructured information that is unlikely to be meaningful to consumers in any event.

Finally, regarding the information that businesses must provide to consumers in response to a right to know request, the Agency should acknowledge the risks related to providing such information in response to a request to know, and also the higher standard of authentication that the CPRA recognizes may be required for more sensitive personal information.[5] Requiring businesses to provide highly sensitive information could expose businesses to increased risk of fraudulent claims and other security breaches, ultimately exposing consumers rather than serving to protect them.

2. Recommendations on Auditing Obligations and Risk Assessments:

A. Audits Performed by the Agency

The Agency should confirm that Agency audits should take place only where there is a credible claim that the business has violated a substantive provision of the CPRA that creates a risk of harm to consumers. Further, the scope of these audits should be limited to the provision(s) alleged to have been violated by the business. Anchoring audits in this manner will maximize the Agency's effectiveness of audits that benefit consumers while also minimizing the compliance burden on businesses. The Agency should also confirm that audits are confidential and are not required to be made public. Adequate protections should also be recognized for privileged and confidential information, including trade secrets and other proprietary and confidential information. The Agency should also confirm that audits should be conducted in a way to avoid access to consumers' personal information.

[4] CPRA Sec. 2, Findings and Declarations.
[5] California Civil Code, § 1798.185.(a)(14).

B. Audits and Risk Assessments Performed by Businesses

(1) 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."

Audits performed by businesses should be protected by strict confidentiality provisions to prevent disclosure to or use by third parties. Relatedly, businesses should not be required to submit work product related to audits to the Agency. A lack of confidentiality under these circumstances would discourage businesses from engaging in a thorough review, thus undermining the goals of the CPRA. Confidentiality provisions would also serve to protect consumers by reducing possible exposure to security breaches in the event that audit information were to fall into the wrong hands. Similarly, businesses should be allowed to perform such audits using internal resources and, if outside auditors are used, should not be required to provide third-party auditors with access to personal information unless strictly necessary, and only under strict controls.

The Agency should also take into consideration the slew of audits and similar reviews to which businesses are already subject, including audits imposed by other laws. In meeting any audit obligations under the CPRA, businesses should have flexibility to use reviews done under other circumstances that advance the same privacy and security goals as the CPRA. This should include audits conducted to maintain industry-standard cybersecurity certifications, such as ISO 27001.

3. Recommendations on Automated Decisionmaking

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

We encourage the Agency to align application of the CPRA to automated decisionmaking with existing privacy laws that also deal with this topic. In particular, we ask the Agency to limit any rules concerning automated decisionmaking to that which produces legal effects or similarly significant effects. For example, the Agency could limit any rules to automated decisionmaking that produces effects regarding a consumer's eligibility for credit, employment, insurance, rental housing, or license or other government benefit.

Such a limitation is consistent with other privacy laws, thus serving consumers' interests without overburdening businesses. For example, Colorado and Virginia's new comprehensive privacy laws govern "profiling" only where profiling is in "furtherance of decisions that produce

legal or similarly significant effects concerning a consumer."[6] Likewise, Articles 15 and 22 of the GDPR provide data subjects with transparency rights in relation to automated decisionmaking only where such decisionmaking produces legal or similarly significant effects. Examples of such decisions include decisions affecting an individual's financial circumstances, such as their credit eligibility, access to health services, consideration for an employment opportunity, or access to education. The limitation to enhanced transparency and choice to decisionmaking that may produce substantial harm to consumers is a limitation that the Agency should likewise recognize. The alternative of providing enhanced transparency and choice in relation to trivial matters would result in overburdening businesses and would not result in providing any meaningful insight for consumers.

Sincerely,

James G. Snell

JGS:rs

[6] *See* Colo. Rev. Stat. § 6-1-306(1)(a)(C); VA. Code Ann. § 59.1-573(A).