From: Jarrell Cook [redacted]
Sent: 11/8/2021 4:40:50 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Andrea Deveau [redacted]; Alicia Priego [redacted]; Lev Sugarman [redacted]; Chandler C. Morse [redacted]
Subject: PRO 01-21 Workday's Preliminary Comments on Proposed CPRA Rulemaking
Attachments: Workday CPRA Rulemaking Comments.pdf

[EXTERNAL]: prvs=79476f3251=[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 Workday's preliminary comments on the proposed CPRA regulations.

Workday Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020

Workday is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics have been adopted by thousands of organizations around the world and across industries—from medium-sized businesses to more than 50% of the Fortune 500.

Workday is pleased to have the opportunity to provide preliminary comments on the proposed rulemaking under the California Privacy Rights Act of 2020. Our comments focus on the following areas: definitions and categories, cybersecurity audits, risk assessments, and automated decision-making.

I. Definitions and Categories

The CPPA should reiterate through definitions and any necessary additional guidance that the regulatory framework it is establishing in this rulemaking does not apply to employee data. At present, employee data is exempted from the scope of the CCPA, with the exemption sunsetting in 2023, on the effective data of the CPRA. This exclusion was intentional, providing the Legislature with time to develop a regulatory scheme for the collection and use of employee data.

The drafters of the CCPA and the CPRA recognized that employee data is collected and used differently than consumer data. For example, employee data is not generally used for marketing, is collected often to comply with laws or fulfill contracts with employees, and often must be kept after the end of the employment relationship to comply with various requirements. Rights of access and deletion can conflict with these obligations, and interfere with required investigations where it is important to keep matters confidential, even where the data relates to the employee.

Given that the CPRA created this window for further legislative activity, it would be premature for the Agency to address employee data in this initial rulemaking.

Should the provision that excludes employee data sunset without adoption of a tailored law addressing Californian's rights over employment-related data, then the Agency should conduct a separate rulemaking exercise directed at employee data, to take account of the differences (including those noted above) between consumer and employee data and how they are collected and used.

Recommendation #1: *Clarify that, consistent with* Cal. Civ. Code § 1798.145(h), *employee data is not contemplated in this rulemaking and may be addressed in 2023, if necessary, by further regulation.*

The CPPA should define the meaning of "significant risk" to consumers' security and consumers' privacy in line with existing and widely-adopted laws and standards. The CPRA has multiple provisions that apply when they involve a "significant risk" to consumers' security and privacy.

CPRA sets out the cybersecurity audit requirement for businesses whose processing of personal information presents "significant risk" to consumers' security. The Agency should define the meaning of "significant risk" in line with existing and widely-adopted laws and standards, such as the NIST Cybersecurity Framework and ISO 27001, ISO 27017, ISO 27018, and FedRAMP. The definition should include due consideration to the size and complexity of the business and the nature and scope of processing activities.

CPRA also requires businesses to submit a risk assessment to the Agency when their processing of consumers' personal information presents a "significant risk" to consumers' privacy. The Agency should adopt the approaches to defining risk seen in other leading privacy and data protection laws, such as the EU's GDPR or Virginia or Colorado's statutes. Processing activities that present a "significant risk" to consumers' privacy under CPRA should be aligned with leading privacy laws, including GDPR, that take a flexible and context-specific approach to best balance privacy interests with the practicality of compliance and enable the regulations to adapt to new and emerging technologies and uses of data.

Recommendation #2: *Define "significant risk" in a manner that is consistent with well-vetted and widely adopted standards to allow for businesses and service providers to easily harmonize their operations and standardize their processes for cybersecurity audits and risk assessments between jurisdictions.*

The CPPA should further clarify that businesses and service providers may combine consumers' personal information that was obtained from different sources for a business purpose to improve their services if they do not monetize consumer data. Building effective machine learning technology depends on large amounts of data—aggregated, de-identified, and combined—being inputted into a system in order for the machine to accurately predict future outputs. While the CPRA sought to restrict the use of data to prevent undisclosed consumer profiling, it did not intend to inhibit the adoption and use of machine learning, and internal uses by the service provider that do not impact individuals' privacy, but improve products and services.

Much of machine learning creates inferences based on large data sets. However, the use of consumer data in this way is not 'profiling' and does not raise the same privacy and equity concerns. This data is not used to market to, make a decision about, or reveal otherwise personal information about an individual. Rather, it is to detect trends and patterns in large data sets to make predictions which, when combined with human judgment, lead to better decisions.

The Agency should allow businesses, including service providers, to combine data to create new and better services when those activities do not monetize consumers' personal information or use it for advertising. This includes combining personal information to help better secure services, make services work better for customers (including services that serve multiple businesses at once), and to mitigate potential risks of bias in machine learning applications. Finally, the CPPA should ensure that any new regulations in this area do not upset the business-service provider relationship and role-based responsibilities established by the CCPA and CPRA that are foundational to effective privacy laws.

Recommendation #3: *Provide guidance that clarifies that businesses, including service providers, are allowed to combine data to create new and better services when those activities do not monetize consumers' personal information or use it for advertising.*

II. Cybersecurity Audits

The CPPA should establish standards for cybersecurity audits conducted in California that are consistent with existing standards and best practices for cybersecurity risk management. At Workday, our top priority is keeping our customers' data secure across all aspects of service. We work closely with international and domestic regulators and standards development organizations to ensure compliance with global privacy regulations. An open, rules-based regulatory framework built on trust is essential to a thriving digital economy.

In a world of increasing cyberattacks, cybersecurity audits are vital to ensuring that personal data isn't compromised. Importantly, what those audits require is a key consideration as well. Any audit standards should be defined by existing, widely-adopted cybersecurity standards such as the NIST Cybersecurity Framework and ISO 27001, ISO 27017, ISO 27018, and FedRAMP, where applicable. These standards have been vetted, proven to address key security risks, and are flexible enough to take account of new threats and developments.

An audit framework divorced from these standards would unnecessarily increase the burden on companies without bringing a corresponding improvement to cybersecurity. Specifically, the CPPA should allow businesses to satisfy the cybersecurity audit requirement by providing certifications and audit reports that demonstrate compliance with existing standards and frameworks, without tying business to prescriptive requirements.

Recommendation #4: *Model CPPA's cybersecurity audit requirements on NIST Cybersecurity Framework and ISO 27001, ISO 27017, ISO 27018, and FedRAMP audit requirements and allow businesses and service providers to satisfy the CPPA's requirements by demonstrating compliance with those established standards.*

III. Risk Assessments

The CPPA should require companies to submit risk assessments only when needed. Conducting regular risk assessments is a key tenet of Workday's proposed approach to a comprehensive privacy framework.

In our experience under a similar regulatory scheme in Europe, the Data Protection Directive, submission of risk assessments that companies conduct should be done on request, rather than on a specific

timeframe. The Data Protection Directive required entities to file records of data processing with data protection authorities. Authorities were inundated with submissions and ultimately did little with them, with enforcement largely driven by complaints. For this reason, even as the General Data Protection Regulation (GDPR) enhanced privacy protections and toughened enforcement, it eliminated the filing requirement.

Given the number of companies subject to CPRA and the amount of data they process, the Agency would be overwhelmed with regular submissions that show good practices and compliant operations, needlessly drawing Agency resources away from more effective tools, like enforcement. The CPPA should take a similar approach and ask for risk assessments when needed for additional action.

Recommendation #5: *Define "regular basis" for risk assessments to be submitted to the CPPA as required in the CPRA to mean 'upon request.'*

IV. Automated Decision-Making

The CPPA should take a narrow approach to developing rules regarding automated decision-making. The CPRA allows for new regulations to be developed to govern "access and opt-out rights with respect to business' use of automated decision-making technology, including profiling," the disclosure of "meaningful information about the logic involved in those decision-making processes," and providing the consumer of "a description of the likely outcome of the process with respect to the consumer."

The regulation of automated decision-making is complex, and needs to protect consumers' rights while not imposing greater burdens than with existing processes. The CPRA was intended to provide consumers with a regulatory framework to preserve their privacy and exercise control over the monetization and sale of their data. The CPRA was not intended to serve as a framework for an extensive regulation on artificial intelligence and machine learning. The Agency should limit the scope of its rulemaking to what is necessary to address Californian's right to make informed choices and exercise their access and opt-out rights when businesses deploy automated decision-making technology.

In this rulemaking, the Agency should focus on identifying how CPRA's access and opt-out rights operate in the context of businesses using automated decision-making technology. For example, mirroring the European Commission Guidelines, rights of access can be limited to non-technical rationale or criteria relied upon to reach a decision, especially if further access would risk exposing sensitive data, IP, or security access points. Rules could also clarify that rights, including opt-out, relate only to automated decision-making producing legal or similar effects concerning individuals that lack any human intervention. Additional limitations could also be helpful, including permitting charging fees for excessive consumer requests.

Potential legislation and regulation on automated decision-making in California has included a broad scope of technologies on a spectrum between simple task automation and truly complex autonomous decision-making. An important first step before wading deep into the regulation of automated decision-

making systems is to identify the scope of systems that are of concern. In this rulemaking, the Agency should limit the scope of its rules to truly fully automated systems whose processes allow for significant decisions to be made without human intervention.

In Workday's whitepaper, 'Building Trust in AI and ML,' we discuss a regulatory framework regarding automated decision-making we encourage California policymakers to adopt. We also encourage the Agency to consider harmonizing any rules it may develop on automated decision-making with the standards and frameworks developed by well-vetted and established international and domestic organizations.

Recommendation #6: *Limit the scope of the CPPA rulemaking to true fully automated decision-making systems and the information consumers need to make informed decisions regarding their right to access and opt out of services deploying automated decision-making systems; and where possible, prioritize harmonization with other regulatory frameworks.*

* * *

Workday appreciates the opportunity to provide preliminary comments to the CPPA on its Proposed Rulemaking under the California Privacy Rights Act of 2020. If you have any questions or if we can provide additional information, please do not hesitate to contact Jarrell Cook, Senior Manager, State and Local Government Affairs, at [redacted].

From: Jennifer Capitolo [redacted]
Sent: 11/8/2021 7:13:08 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 - Comments from California Water Association
Attachments: PRO 01-21 California Water Association Preliminary Comments on CPRA Proposed 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.

Dear Ms. Castanon,

On behalf of the California Water Association, attached please find our comments for the California Privacy Rights Act preliminary comment period. We look forward to engaging with you and your staff as you work to implement the CPRA.

Take care…JMC

JENNIFER M. CAPITOLO Executive Director @ California Water Association
601 Van Ness Avenue, Suite 2047, San Francisco, CA 94102
[redacted] (c)

Working Together.
Achieving Results.

California Water Association

VIA EMAIL

November 8, 2021

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

Dear California Privacy Protection Agency:

On behalf of California Water Association ("CWA"), we provide these comments on the proposed rulemaking under the California Privacy Rights Act ("CPRA"). CWA is the statewide association representing the interests of investor-owned water utilities subject to the regulatory jurisdiction of the California Public Utilities Commission ("CPUC"). CWA's members provide safe, reliable, high-quality drinking water to approximately six million Californians. CWA appreciates the opportunity to comment on the proposed regulations and assist in providing greater clarity to businesses and consumers with respect to CPRA implementation.

Investor-owned water utilities provide an essential public service under close regulatory oversight by the CPUC governing all virtually aspects of their services, rates, and operations. In providing such essential public service, water utilities must collect, use, and retain certain personal information of their customers consistent with the requirements specified by the CPUC and other regulatory agencies. There is a need for consistency between the regulations implementing the CPRA with respect to water utilities and the statutory and regulatory requirements enforced by the CPUC.

1. **Introduction**

Approved as a ballot measure in November 2020, the CPRA expanded the scope of the California Consumer Privacy Act of 2018 ("CCPA"). The CCPA created a range of consumer privacy rights and business obligations with regard to the collection and sale of personal information. The CPRA amends and expands the CCPA, establishing further consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. To implement the law, the CPRA established the California Privacy Protection Agency ("Agency") and vested it with the "full administrative power, authority and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018."

Executive Director
Jennifer Capitolo
California Water Association
601 Van Ness Avenue, Suite 2047
San Francisco, CA 94102-6316
415.561.9650
415.561.9652 fax
[redacted]
www.calwaterassn.com

Administrative Director
Elizabeth Caldwell
California Water Association
700 R Street, Suite 200
Sacramento, CA 95811
916.231.2147
916.231.2141 fax
[redacted]

CWA Billing Address
California Water Association
700 R Street, Suite 200
Sacramento, CA 95811

CWA Mailing and Shipping Address
California Water Association
601 Van Ness Avenue, Suite 2047
Mail Code: #E3-608
San Francisco, CA 94102-3200

The Agency's Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 invites stakeholders to submit comments concerning related to any area on which the Agency has authority to adopt rules. The Agency also identified specific topics and questions as to which it is particularly interested in receiving views and comments. CWA appreciates this opportunity to provide input on this important topic and provides the following comments regarding the Agency's identified topics and questions.

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

CPUC General Order 103-A[1] established minimum standards for design, construction, location, maintenance, and operations of the facilities of water and wastewater utilities operating under the jurisdiction of the CPUC. General Order 103-A also sets forth requirements for record retention. Pursuant to General Order 103-A, certain records, which include records containing personal customer information, must be retained for at least ten years, and longer in certain circumstances.

a. Requests to Delete

In order to comply with General Order 103-A, water utilities are not in a position to grant customer requests under the CCPA to delete customer-specific information unless the CPUC no longer requires its retention. At this point in time, these records may have been moved to offsite storage or may be in difficult to manage formats, such as tape logs. The burden of locating and deleting these records would far outweigh any public benefit. CWA therefore requests that historical water utility records more than ten years old be exempt from deletion request obligations. CWA suggests that the Agency's proposed rulemaking include revisions to the Attorney General's Regulations concerning the customer's right to delete under the CCPA and proposes the following language be incorporated into the final regulations:

> *§ 999.313(d)(3). Responding to Requests to Delete*
>
> *If a business stores any personal information on archived or backup systems or at an offsite storage location, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system or at an offsite storage location, until the archived or backup system or offsite storage location is next accessed or used. Personal information located on archived or backup systems or in an offsite storage location that is more than 10 years old at the time of the request shall be exempt from the CCPA's deletion requirement as set forth in Civil Code section 1798.105.*

[1] General Order 103-A is available at https://docs.cpuc.ca.gov/PublishedDocs/PUBLISHED/GRAPHICS/107118.PDF.

Alternatively, since the Attorney General's regulations already contemplate delaying compliance with consumer requests to delete information on archived or backup systems, CWA requests that they be modified to account for the difficulties associated with accessing historical water utility records that may contain personal information. CWA suggests the following alternative language be incorporated into the Agency's regulations:

> *§ 999.313(d)(3). Responding to Requests to Delete (alternative proposed language)*
>
> *If a business stores any personal information on archived or backup systems or at an offsite storage location, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system or at an offsite storage location, until the archived or backup system or offsite storage location is next accessed or used. If a business does not access its archived or backup systems or its offsite storage location within twelve (12) months of a consumer's request to delete, the deletion request shall expire. Businesses shall provide notice to consumers of the possibility of expiration of requests for deletion of personal information on archived or backup systems or at an offsite storage location.*

b. Requests to Correct

Similarly, water utilities' compliance with General Order 103-A could potentially conflict with the utilities' compliance with rules concerning the new right to correct established by the CPRA. The CPRA tasks the Agency with rulemaking concerning how often, and under what circumstances, a consumer may request a correction to their personal information. *See* Civil Code, § 1798.185(a)(8). The Agency also specifically requested input concerning 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. Civil Code, § 1798.185(a)(8)(A).

CWA suggests that the Agency adopt rules limiting consumer requests for correction to data obtained or sold by the business during the 12-month period preceding the request for correction. This limitation would mirror the 12-month period provided by the CCPA for disclosure requests. Civil Code, § 1798.130. Furthermore, a time limitation would prevent the disproportionate burden on businesses, like water utilities, that are required to retain customer personal records for significant periods of time. As these personal records age, the customer information contained within is more likely to become inaccurate due to being out-of-date. As water utilities already retain outdated customer information to comply with General Order 103-A and do not sell this customer information in the ordinary course of business, there is likely to be little to no harm associated with incorrect

information being retained when it is more than 12 months old.

Alternatively, as the CPRA already contemplates exceptions to the requirement to respond to consumer requests for correction under Civil Code, § 1798.185(a)(8)(A), CWA suggests that the Agency develop rules allowing that businesses be exempted from the obligation to take action on a request when the data was not acquired or sold in the past 12 months and will not be used for commercial purposes.

3. **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 CPUC has authorized water utilities to release certain customer-specific information to local governments, wholesale water agencies, and other entities for the purpose of calculating local taxes, managing wastewater systems, collecting miscellaneous fees, and implementing and enforcing conservation programs and measures. The transfer of this customer-specific information thus serves important public policy interests. The CPUC has established safeguards that ensure that the customer information that is shared is only used for the purpose for which it is intended and is not further disclosed.

Although some water utilities may collect a nominal fee related to the transfer of data to a neighboring municipality or wastewater utility, they do not "sell" data in the manner for which the CCPA was designed to provide protection. The fees collected by the water utilities simply shift the financial burden and costs of accumulating and transferring the data to the party receiving the information rather than the utility's customers. The opt-out provisions in the CCPA and the proposed regulations should not apply to this type of data collection and sharing by water utilities since the information is not being used by the water utilities for commercial purposes, but instead to serve a public purpose.

As the CPRA now provides for additional rulemaking to update the CCPA rules on the right to opt-out of the sale of personal information, CWA recommends that the Agency update the Attorney General's regulations concerning the right to opt-out to include the following language:

> *§ 999.301. Definitions*
>
> *"Sell," "selling," "sale," or "sold" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration as set forth in Civil Code section 1798.125(b) and specified in these regulations. The transfer of a consumer's personal information by a regulated public utility to a state or local government agency or district or another regulated public utility, as authorized by the California Public Utilities*

Commission, is not a "sale" under Civil Code section 1798.140(v), notwithstanding an exchange of monetary compensation for such transfer.

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

The CPUC has authorized and, in some cases, requires that water utilities use and share customer-specific data that may constitute "sensitive personal information" under the CPRA. Use and sharing of customer-specific data under CPUC safeguards should be permissible notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information. The CPUC authorizes this data-sharing under specific safeguards, which protect the consumer from use and disclosure of personal information for commercial purposes.

As this data sharing is non-commercial and used to promote statewide policy goals, such as water conservation, under the CPUC's supervision, it is exactly the type of use or disclosure that should be permissible notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information. CWA recommends that any regulations promulgated by the Agency under Civil Code, § 1798.185(a)(19)(C) should clarify that use or disclosure of a consumer's sensitive personal information by water utilities under CPUC supervision should be permissible notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information.

CWA recognizes the challenge of balancing consumer privacy interests against the CPUC's mandate to ensure safe, reliable and affordable utility service, and the obligation of regulated water utilities to comply with CPUC requirements and directives. CWA appreciates the opportunity to submit these comments.

Respectfully submitted,

[redacted]

Jennifer Capitolo
Executive Director
California Water Association

From: =Jay [redacted]
Sent: 11/9/2021 10:38:58 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: GCA3 - CPPA CPRA Invitation for Preliminary Comments.pdf

[EXTERNAL]: [redacted]

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

Dear Ms. Debra Castanon,

We held an informal gathering last week of various authorized agencies that are already submitting opt-out consent requests and other requests to businesses on behalf of consumers in various industries. There were many great insights and common issues that came up, and there was consensus to supply you with a submission of them for your "Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act Of 2020".

I left you voice mail that we sent it via USPS and you should receive it in the coming days. But, in the interest of respecting your time and helping you by including these thoughts as you synthesize contributions in the coming days, we thought it might be helpful to submit a copy of it to you here electronically as well. We are all grateful for the work you are doing, and for working with us on the timing of this submission as we only met for the first time last Thursday, and yet the contributions did seem insightful and hopefully helpful for your efforts.

Please feel free to contact me if there are any questions.

Cheers!

=Jay

PHONE: [redacted]
EMAIL: [redacted]
WEB: privacy.coop
LOCATION: Dallas, TX

November 8, 2021

On Behalf of various gathered Authorized Agents

To:

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

Dear Ms. Debra Castanon,

We are an informal group of Authorized Agents (AAs) that represent consent elections of various people, and we are gathering to understand better our common needs and pain-points, attempting to understand better any common solutions that might help everyone. Our insights may prove valuable as individually our respective organizations daily wrestle with representing data subject consent requests to companies in different industries. While we are just now identifying more AAs, there are currently eight such organizations and the list is likely to grow in the coming months. In an early discussion, the following thoughts were raised, and we'd like to submit them now per your open request for comment.

The invitation asks interested parties to comment on, "How businesses should process consumer rights that are expressed through opt-out preference signals." (See Civil Code, §§ 1798.135 and 1798.185(a)(20).)

Businesses are responding differently to different AA requests – often rejecting some AA requests for opt-outs and directing AAs to tell those whom they represent to individually abandon their AA and just use resources provided by the company in question. Often, they do so in the name of "privacy of the data subject" and in some cases, these businesses have subsequently sent out in open CC'd emails to *all* listed data subjects in the request, exposing what had been each data subjects' private request to all the others. The sited resources and steps to follow to opt-out are routinely different from company to company, and the bar of finding, comprehending, and acting upon each company's unique process of how to use these resources often proves too high for the average person to approach—which is likely the original reason for using an AA in the first place. In some cases, these businesses are asking for 10 or more SPI or PII data to *prove* identity before they will consider agreeing to comply with the request, such as social security numbers, street addresses, drivers license numbers, and the like.

For consideration, CA § 999.315(h)(4) states "The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request." We have found that in most cases a simple email address, phone number, or account number is sufficient for most modern companies to identify the data subject's information.

Historically, if we consider broader regulatory efforts predating the internet, businesses are not required to verify that the person submitting an opt-out request is really even the consumer for whom the business has personal information. Opt-outs have historically enjoyed the lowest bar of requirement for consent election notifications. For example, one long-standing telco ruling found that even if a neighbor takes a postcard out of another's mailbox, checks opt-out on it, and sends it in, the telco must honor

that opt-out without any further question. Compliance should fall on the side of the consumer and not the business – especially for "secondary purposes" of data processing and sales not required for the primary product/service.

A common form of sale and sharing of consumer personal information is auction-based advertising that takes place entirely within an auction market hosted by a single social media company. Such an auction is carried out by software-implemented "bidders" that carry out individual advertising campaigns for different businesses.

After a consumer has opted out of the sale or sharing of their personal information, the CPRA requires that such information no longer be "sold" where "sold" is defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."

Markets are, by their nature, information transfer tools. This is just as true of markets within a social media platform as it is of any other market. When multiple advertisers participate in the same social media advertising platform, each advertiser that transfers customer personal information into the system receives valuable consideration from the other advertisers. For example, consider a vendor of health education materials that transfers a customer list to a social media platform, and uses the customer list as an "exclusion list," to avoid showing its ads to existing customers. After the exclusion list is set up, a California consumer whose personal information is on the list opens a social media app and causes an ad auction to happen. Because the health education vendor is excluded from bidding, a seller of fraudulent medical devices wins the ad auction. Although the social media platform represented itself as a service provider to both businesses, the auction resulted in a "sale," as defined by the law, of personal information from one advertiser to the other. Similarly, a list of personal information used as a targeting list can result in information transferred from one business to another, as a price signal.

The law clearly does not exclude auction-based advertising internal to a social media platform from the scope of "sale or sharing." Future regulations should make it clear that personal information that pertains to a person who has opted out may not be transferred in such a way that it can be used in any internal auction on a social media platform, including as part of any "custom audience" or targeting list.

This gathering of AAs respectfully submits these suggestions and will gladly consider providing further details as requested.

Sincerely,

J. Oliver Glasgow

From: Anthony Stark [redacted]
Sent: 11/8/2021 9:54:23 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Hannah Zimmerman [redacted]; Bubba Nunnery [redacted]
Subject: PRO 01-21 - ZoomInfo Comments Regarding CPRA Regulations
Attachments: CPRA Comments Letter - ZoomInfo (11.8.21).pdf

[EXTERNAL]: [redacted]

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

Dear California Privacy Protection Agency:

Please see the attached correspondence reflecting our initial comments on the CPRA regulations.

Warm regards,

Anthony Stark
General Counsel

O: [redacted]
E: [redacted]

805 Broadway Street, Suite 900
Vancouver, WA 98660

zoominfo.com

zoominfo

November 8, 2021

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

Dear California Privacy Protection Agency,

ZoomInfo is grateful for the opportunity to submit these comments as part of the rulemaking process for the California Privacy Rights Act (CPRA). We are a software and data intelligence company that provides information for business-to-business sales and marketing. We support consumer privacy rights and believe that, in large part due to the work of this Agency, we are on the path to developing a healthy privacy framework for the State of California (and beyond).

From the prompts provided, we have selected a handful of issues on which we wish to express our views:

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

We propose following the GDPR, which provides that these terms apply where the automated decisionmaking or profiling *produces legal effects concerning an individual or that similarly significantly affects the individual.* For example, automated decisionmaking or profiling may impact an individual's ability to get credit, insurance, housing, or employment. Unless such decision-making or profiling has a significant effect on the individual, we do not think it should create heightened obligations on businesses, because such heightened obligations would not meaningfully help consumers.

Innovated technologies may use automated decisionmaking technology in ways that are neutral or have no significant impact with respect to consumer privacy. Businesses may use such technologies to improve their products, services, and business processes in ways that benefit consumers or increase efficiency. We should not place roadblocks in the way of innovation unless it would create a real benefit to consumer privacy. In addition, we think aligning the CPRA with the GDPR where it is reasonable to do so provides clear benefits in terms of predictability for businesses, reducing compliance costs, and increasing compliance rates.

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

We propose that the obligation to respect opt-out preference signals be limited to information a business receives through the same technology delivering the preference signal. In other words, if the signal is delivered through a setting on a web browser, a business's obligation should extend only to information obtained through that browser. We are concerned that businesses would otherwise have an unreasonable (and in some cases impossible) task of trying to match personal information received from one source with data about an individual otherwise in its possession.

For example, the information accessible through a web browser may be limited to an IP address and device information. It may be virtually impossible to know that this constitutes personal information of another person whose information the business possesses.

Honoring the opt-out with respect to only that browser information is still very useful: it would still serve to ensure that businesses do not share such information via cookies or some similar means with, for example, third-party analytics or ad placement providers. And limiting the scope will also avoid placing undue pressure on businesses to create ways to tie data sets together when it would be impractical and even counterproductive to do so.

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

We suggest the Agency update the categories of "personal information" to add an exclusion of business contact information. Business contact information means the information people typically put on a business card: name, company, title, work phone, and email. This kind of information is not generally considered sensitive or private. For decades, directories have existed that include contact information, and they provide an important function in fundraising, campaigning, sales, marketing, and recruiting, among other things. Tens of millions of business professionals readily share this information every day, by passing out business cards, posting it on company websites, or publishing it on professional networking sites like LinkedIn.

Business contact information is used by every business in California to market and sell their products and services to other businesses, to engage in recruiting, and similar purposes. It is a hugely important part of the economy that many people simply do not see. Business-to-business transactions represent approximately $26 trillion annually in the U.S., nearly twice the transaction value of all consumer spending. It is important that we do not disrupt the ability of companies to use this vital information and thereby create unnecessary friction in our economy, especially while small businesses and startups are still struggling with the impact of the pandemic, and remote communication and selling has become even more important.

Recognizing these distinctions by defining and exempting business contact information from the definition of "personal information" will help ensure that the focus of the CPRA remains squarely on protecting consumers without unduly regulating the nonsensitive information that businesses need to efficiently go to market and engage in routine business-to-business communications and transactions.

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

We suggest the Agency update the categories of "sensitive personal information" to exclude the contents of emails in an employment, business, or professional capacity. Generally speaking, an individual has no expectation of or right to privacy when sending or receiving email using a company-owned domain and company email servers. If we include those communications within the definition of sensitive personal information, a business's need to conduct its business, including

ensuring compliance with applicable law and company policy, would be potentially in conflict with the statute.

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.

We suggest that the contents of email sent to or from a business email account or primarily used for business or professional purposes should not be subject to the right to limit use and disclosure. Not only is this information not used to infer characteristics about a consumer, but allowing individuals to limit the use and disclosure of their emails would impair the ability of businesses to operate.

Thank you for your consideration. Please feel free to contact me if you have any questions.

Sincerely,

[redacted]

Anthony Stark
General Counsel
ZoomInfo
[redacted]

From: Ross Teixeira [redacted]
Sent: 11/9/2021 4:16:31 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Castanon, Debra@CPPA [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b9766af8eba04290bfa5ae3e150c60e7-Castanon, D]
Subject: Re: CPPA PRO 01-21 Comments Submission: Princeton University Center for Information Technology Policy
Attachments: CITP CPRA Comments CORRECTED.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 Ms. Debra Castanon,

Please use our CORRECTED comments from Princeton's Center for Information Technology Policy instead of our original submission, attached.

Thanks,

Ross Teixeira
PhD Computer Science
Princeton University
[redacted]

Il 9 nov 2021, 2:50 AM -0500, Regulations <Regulations@cppa.ca.gov>, ha scritto:

> Thank you for submitting a comment to the California Privacy Protection Agency. This e-mail inbox is intended for receiving written comments and this is an automated reply. If you have a question, please write to info@cppa.ca.gov or follow the instructions in the Invitation for Comments. Please go to https://cppa.ca.gov/regulations/%C2%A0for updates on the Agency's rulemaking activities.

PRINCETON UNIVERSITY

CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

November 8, 2021

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

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

Thank you for the opportunity to provide preliminary comments to the California Privacy Protection Agency ("Agency") on proposed rulemaking regarding the California Consumer Privacy Act ("Act"), as amended by the California Privacy Rights Act.

We are academic researchers associated with the Center for Information Technology Policy ("CITP") at Princeton University, with expertise in computer science, law, and public policy.[1] Our comments narrowly focus on how the Agency can protect consumer privacy by improving how businesses implement data access rights that are guaranteed to consumers.[2] We are currently conducting an academic study of how businesses implement data access rights, and our preliminary observations indicate significant shortcomings in current practices.

While not the focus of our comments, we also encourage the Agency to consider clarifying the Act's applicability to Internet Protocol addresses and third-party online tracking. We previously addressed these topics in comments to the California Department of Justice, and for brevity we do not repeat our views here. *See* Comments on Revised Proposed Regulations Implementing the California Consumer Privacy Act, CITP, Feb. 25, 2020 (3-6).[3]

---

[1] In keeping with Princeton's tradition of service, CITP's faculty and students provide nonpartisan research, analysis, and commentary to policy makers, industry participants, journalists, and the public. These comments reflect the independent views of the undersigned scholars.

[2] While our comments focus on data access rights as the topic of our current research, our comments apply equally to other consumer rights afforded by the Act, including data deletion rights, data correction rights, and rights to opt-out of data sharing and sale.

[3] Available at https://citpsite.s3.amazonaws.com/wp-content/uploads/2020/02/27164209/CITP-Clinic-CCPA-Comments-2.pdf

1. **Improve the discoverability of data access rights.**

In order for consumers to exercise data access rights, consumers must be aware of those rights and how to invoke them. Our ongoing research shows, consistent with prior work, that businesses use a variety of methods for accepting data access requests that obstruct consumer understanding of those rights. While these business practices might be consistent with current regulations implementing the Act, they pose a significant risk of consumer confusion because of vague descriptions and inconsistent presentation across different online services.[4] Furthermore, many online services require a consumer to navigate through several pages or lengthy text to learn about how to exercise data access rights.

We encourage the Agency to consider how to improve the discoverability of data access rights. One approach would be to harmonize discoverability requirements for all of the data rights guaranteed by the Act, drawing on how online services are required by current regulations to promote discoverability of opt-out rights (e.g., "Do Not Sell My Personal Information" links). Another approach would be to articulate lightweight technical requirements for standardized data rights discoverability (e.g., well-known URLs), analogous to the Global Privacy Control that the Agency is considering for promoting usability of opt-out rights.

2. **Improve the usability of data access rights.**

There are significant benefits to consumers from straightforward and consistent procedures for exercising their data access rights. Our in-progress research has highlighted, again consistent with prior work, that the user experience of submitting data access requests is inconsistent among businesses and often unnecessarily burdensome. Some businesses, for example, require that consumers fill out a PDF document to make a request. Other businesses require consumers to create a new account with a service provider that manages data rights requests.

Excessive authentication requirements are a particularly common form of unnecessary burden on consumer data access rights. We have observed a number of online services that require a driver's license scan, an additional telephone number verification, or an additional email verification. These authentication requirements can

[4] Hana Habib et al., "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices, ACM CHI '20. Available at https://usableprivacy.org/static/files/habib_chi_2020.pdf

have little security rationale when considering the service's ordinary login process and the sensitivity of the data at issue.

Another shortcoming of current implementations is that businesses can mishandle consumer requests. We have found several instances of incorrectly configured email mailboxes, such that the businesses automatically reject all consumer data rights requests. We have also observed instances of businesses providing untimely responses to data access requests because of overly aggressive email spam filtering. Since data rights request emails can be formulaic, especially when using public templates for submitting requests, there is reason to believe that spam filtering can be a common issue for processing by businesses.

Yet another issue we identified is that some businesses expressly decline to answer clarifying questions about how to exercise data access rights. We found that these businesses would only process (or decline to process) a formal request for customer data. As a point of comparison, the European Union's General Data Protection Regulation provides in Article 12 and Recital 59 that businesses must "facilitate" the exercise of consumer data rights.

We encourage the Agency to consider improvements to the usability of the data access rights guaranteed by the Act. In particular, we encourage the Agency to consider requirements that (1) if a business maintains an existing user account system it must (absent good cause) allow consumers to make data access requests online using their ordinary accounts; (2) a business must regularly test its data access request process and report any significant errors to the Agency; and (3) a business must respond to reasonable consumer inquiries about processes for exercising data access rights.

3. Improve the security of data access rights.

We have found that some businesses use inadequate technical safeguards and business process protections in their data access rights processes, risking unauthorized disclosure of consumer data. Prior work has made similar observations.[5] These shortcomings are particularly acute for processes that rely on email, which may not apply modern email verification protocols, as well as processes that rely on device identifiers, which may not use identifiers that are intended for authentication. Given the sensitive nature of these vulnerabilities, we would welcome the opportunity to brief the Agency about our preliminary findings.

---

[5] Di Martino and Robyns, Personal Information Leakage by Abusing the GDPR "Right of Access", SOUPS '20. Available at https://www.usenix.org/system/files/soups2019-di_martino.pdf

* * *

We appreciate the opportunity to provide preliminary comments and are available to answer any questions the Agency may have.

Respectfully submitted,

Gunes Acar
Assistant Professor of Computer Science, Radboud University

Mihir Kshirsagar
Technology Policy Clinic Lead, Center for Information Technology Policy, Princeton University

Jonathan Mayer*
Assistant Professor of Computer Science and Public Affairs, Princeton University

Ross Teixeira*
Graduate Student, Department of Computer Science, Princeton University

* denotes principal comment authors.

Contact:

Website: https://citp.princeton.edu
Phone: [redacted]
Email: [redacted]

From: Jacob Favre [redacted]]
Sent: 10/22/2021 9:22:55 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21

[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.

In regards to opt-outs on websites. Why do you allow websites to show you an opt-out consent form and when you select to opt-out of everything, why do you allow websites to still send data off to 3rd party vendors?

That seems to be a clear violation of your regulations. When I opt-out, I do not want any data to leave my browser to go to the very places I asked to be opt-ed out of.

- thanks
Jacob

From: Ross Teixeira [redacted]
Sent: 11/8/2021 11:50:00 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: CPPA PRO 01-21 Comments Submission: Princeton University Center for Information Technology Policy
Attachments: CITP CPRA Comments.pdf

[EXTERNAL]: [redacted]

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

Dear Ms. Debra Castanon or whom it may concern,

We are academic researchers associated with Princeton University's Center for Information Technology Policy (CITP). We thank you for the invitation to submit comments on PRO 01-21, Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020.

We are actively conducting research on data rights requests under the California Consumer Privacy Act. Based on our preliminary results, we submit the attached comments for review. We are available to answer any questions the California Privacy Protection Agency may have.

Thank you,

Ross Teixeira
PhD Computer Science
Princeton University
[redacted]

PRINCETON UNIVERSITY

CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

November 8, 2021

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

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

Thank you for the opportunity to provide preliminary comments to the California Privacy Protection Agency ("Agency") on proposed rulemaking regarding the California Consumer Privacy Act ("Act"), as amended by the California Privacy Rights Act.

We are academic researchers associated with the Center for Information Technology Policy ("CITP") at Princeton University, with expertise in computer science, law, and public policy.[1] Our comments narrowly focus on how the Agency can protect consumer privacy by improving how businesses implement data access rights that are guaranteed to consumers.[2] We are currently conducting an academic study of how businesses implement data access rights, and our preliminary observations indicate significant shortcomings in current practices.

While not the focus of our comments, we also encourage the Agency to consider clarifying the Act's applicability to Internet Protocol addresses and third-party online tracking. We previously addressed these topics in comments to the California Department of Justice, and for brevity we do not repeat our views here. *See* Comments on Revised Proposed Regulations Implementing the California Consumer Privacy Act, CITP, Feb. 25, 2020 (3-6).[3]

---

[1] In keeping with Princeton's tradition of service, CITP's faculty and students provide nonpartisan research, analysis, and commentary to policy makers, industry participants, journalists, and the public. These comments reflect the independent views of the undersigned scholars.

[2] While our comments focus on data access rights as the topic of our current research, our comments apply equally to other consumer rights afforded by the Act, including data deletion rights, data correction rights, and rights to opt-out of data sharing and sale.

[3] Available at https://citpsite.s3.amazonaws.com/wp-content/uploads/2020/02/27164209/CITP-Clinic-CCPA-Comments-2.pdf

1. **Improve the discoverability of data access rights.**

In order for consumers to exercise data access rights, consumers must be aware of those rights and how to invoke them. Our ongoing research shows, consistent with prior work, that businesses use a variety of methods for accepting data access requests that obstruct consumer understanding of those rights. While these business practices might be consistent with current regulations implementing the Act, they pose a significant risk of consumer confusion because of vague descriptions and inconsistent presentation across different online services.[4] Furthermore, many online services require a consumer to navigate through several pages or lengthy text to learn about how to exercise data access rights.

We encourage the Agency to consider how to improve the discoverability of data access rights. One approach would be to harmonize discoverability requirements for all of the data rights guaranteed by the Act, drawing on how online services are required by current regulations to promote discoverability of opt-out rights (e.g., "Do Not Sell My Personal Information" links). Another approach would be to articulate lightweight technical requirements for standardized data rights discoverability (e.g., well-known URLs), analogous to the Global Privacy Control that the Agency is considering for promoting usability of opt-out rights.

2. **Improve the usability of data access rights.**

There are significant benefits to consumers from straightforward and consistent procedures for exercising their data access rights. Our in-progress research has highlighted, again consistent with prior work, that the user experience of submitting data access requests is inconsistent among businesses and often unnecessarily burdensome. Some businesses, for example, require that consumers fill out a PDF document to make a request. Other businesses require consumers to create a new account with a service provider that manages data rights requests.

Excessive authentication requirements are a particularly common form of unnecessary burden on consumer data access rights. We have observed a number of online services that require a driver's license scan, an additional telephone number verification, or an additional email verification. These authentication requirements can

[4] Hana Habib et al., "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices, ACM CHI '20. Available at https://usableprivacy.org/static/files/habib_chi_2020.pdf

have little security rationale when considering the service's ordinary login process and the sensitivity of the data at issue.

Another shortcoming of current implementations is that businesses can mishandle consumer requests. We have found several instances of incorrectly configured email mailboxes, such that the businesses automatically reject all consumer data rights requests. We have also observed instances of businesses providing untimely responses to data access requests because of overly aggressive email spam filtering. Since data rights request emails can be formulaic, especially when using public templates for submitting requests, there is reason to believe that spam filtering can be a common issue for processing by businesses.

Yet another issue we identified is that some businesses expressly decline to answer clarifying questions about how to exercise data access rights. We found that these businesses would only process (or decline to process) a formal request for customer data. As a point of comparison, the European Union's General Data Protection Regulation provides in Article 12 and Recital 59 that businesses must "facilitate" the exercise of consumer data rights.

We encourage the Agency to consider improvements to the usability of the data access rights guaranteed by the Act. In particular, we encourage the Agency to consider requirements that (1) if a business maintains an existing user account system it must (absent good cause) allow consumers to make data access requests online using their ordinary accounts; (2) a business must regularly test its data access request process and report any significant errors to the Agency; and (3) a business must respond to reasonable consumer inquiries about processes for exercising data access rights.

3. Improve the security of data access rights.

We have found that some businesses use inadequate technical safeguards and business process protections in their data access rights processes, risking unauthorized disclosure of consumer data. Prior work has made similar observations.[5] These shortcomings are particularly acute for processes that rely on email, which may not apply modern email verification protocols, as well as processes that rely on device identifiers, which may not use identifiers that are intended for authentication. Given the sensitive nature of these vulnerabilities, we would welcome the opportunity to brief the Agency about our preliminary findings.

---

[5] Di Martino and Robyns, Personal Information Leakage by Abusing the GDPR "Right of Access", SOUPS '20. Available at https://www.usenix.org/system/files/soups2019-di_martino.pdf

* * *

We appreciate the opportunity to provide preliminary comments and are available to answer any questions the Agency may have.

Respectfully submitted,

Mihir Kshirsagar
Technology Policy Clinic Lead, Center for Information Technology Policy, Princeton University

Jonathan Mayer*
Assistant Professor of Computer Science and Public Affairs, Princeton University

Ross Teixeira*
Graduate Student, Department of Computer Science, Princeton University

* denotes principal comment authors.

Contact:

Website: https://citp.princeton.edu
Phone: [redacted]
Email: [redacted]

From: Michael Weed [redacted]
Sent: 10/27/2021 12:33:53 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 CCPA/CRPA Comments

[EXTERNAL]: prvs=89344c8b77=[redacted]

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

Please see my comments below each key area that the CPRAA is requesting comments on.

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

a. A business's processing is a significant risk then the business requests personally identifiable information (PII), wherein the information can be tied back to an individual; and where businesses request payment information, such as credit cards, bank accounts, retirement accounts, stock accounts, and other similarly related items that can potentially cause great loss to individuals if the information was leaked.

b. Businesses that must perform yearly audits should release two reports: an external report showing the number of systems an individual's information is kept in, for how long that info is kept and what triggers deleting it, how many employees and contractors have access to that information, and what processes are used to protect the information (such as passwords with 15+ characters, multifactor authentication, and firewalls); and an internal report detailing who in a business specifically has access to customer information, details on security layers to help with 3rd-party audits, a system chart which shows how each system connects to allow for visual understanding of where data can flow, and finally details on the number of times an attempted breach was logged. Maintaining independent audits of a business should require using a state or federally-authorized auditor that does not have ties to the business or to foreign governments.

c. Businesses should submit both the internal report and the external report to the CPRAA so that in case of a breach in the subsequent year, the CPRAA can act quickly with the information provided by the audits. Risk assessments should be sent once a year for all businesses, and twice a year for businesses performing in excess of $10,000,000 in revenue or spending yearly. The cost of these assessments and audits will tell the business if it is worth processing customer information, or if the business should cut that out entirely and thus remove the need for audits.

d. Risk to privacy outweighs the benefits when a customer's personal information is not used to process an order for a customer. A company should collect information only when fulfilling a service, such as collecting billing and shipping address to process and ship an order to a customer. A company should not collect data on a customer just because the company does not trust the customer, such as a social media company requiring picture ID because the social media company does not believe the person's name. This is not being used to process an order, and therefore the social media company or any other company should not be allowed to request this information.

2. Automated Decisionmaking

a. Any process that takes less than 7 seconds to complete should be considered automated decisionmaking. Human reaction speed can typically be 0.5 – 1.5 seconds and therefore anything that takes only a few seconds is being done through automated processes. This includes collecting device and behaviorally information without the assistance of a human.

b. Customers should be made aware of any automated decisionmaking that affects either their ability to use businesses services, or will affect their future ability to use the current services. It should not be hidden 10 pages into a Terms of Services Agreement. Consumers should know why they were rejected, if the business rejects them for services.

c. After confirming a match from the customer to the customer's data, businesses should provide any and all relevant decisionmaking that affected that customer specifically. The business does not have to explain how it affects other customers, but the business should be able to express how it affects the customer that requests information. The information should be expressed in basic but correct terms, with as little jargon as possible. Individuals should be made aware of why they were denied for services, if denied.

d. Consumers should be able to opt-out in one click or the press of a button for automated profiling. Automated decisionmaking that helps a business process customer applications or orders should be noted to the customer, but if the decisionmaking process declines a customer, the customer should be able to request a manual review. When systems such as Applicant Tracking Systems (ATS) are used to deny an individual automatically, individuals should be able to request a manual review.

3. Audits Performed by the Agency

a. The CRPA should have authority to investigate business audits, systems and physical security, machines and servers used to transmit or hold data, and the conversations or process by which individuals have requested their information, requested deletion, et cetera.

b. The CRPA should audit 1% of qualified businesses annually by placing all businesses on a list, sorted by company size, and starting at the 100th percentile, 75th percentile, 50th percentile, and 25th percentile listed companies, auditing them, and then going down the list. This will ensure companies of all sizes are held accountable. The CRPA should also be able to audit an additional 1% of companies on the basis of individual or consumer group reports. This additional 1% audits should be performed on the self-reports that appear to be the most potential for damage.

c. You cannot simultaneously safeguard information and also conduct an audit. Today's systems are not built with that in mind but likely will arise as these regulations begin to take effect. Best-case scenario is having the auditor perform audits with business staff to ensure correct visibility, but the business staff could steer auditors in the wrong direction to hide abuse or missteps by the business.

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

a. Consumers should have the right to request correction of their information and if done correctly, businesses should then comply within 48 hours or same-day if the business processes applications such as for loans or banking services.

b. Consumers should be able to update information as often as they require.

c. Requests by consumers for information updating should provide both the personal information that is inaccurate, and what the information should be. The consumer request should provide relevant details that only the true, or "real", consumer would know in relation to the business' related services and the information the business already has captured on the consumer.

d. Businesses should be inclined to resolve all legitimate mistakes or errors of submission, whether by unintentional user error or by system error. Businesses should not be obligated to update information that is repeatedly and willfully given that proves to be false or untrue information.

e. Businesses should be required to update legitimate errors, so customers should not have rights to a written addendum.

5. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information

a. Businesses should allow a customers to opt out of the sale of their data in less than 30 seconds by phone, in less than 3 clicks on the business website, or by a simple one line message from email, chat, or text.

b. Businesses should have at least two different opt-out methods that specifically relate to the services. For example, a social media company that is an online-first business should not require sending physical mail to opt-out.

c. Businesses should not be allowed to target minors in selling their data

d. A business should be able to complete opt-out within 7 business days of receipt of confirmation of opt-out

e. If consumers want to re-opt-in for data selling, they should create a new account with the business

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

a. "Sensitive Information" should be defined as any characteristic that can be studied; or any information that cannot be easily changed such as height, ethnicity, origin, social security number, of bank account number.

b. Information should be disclosable when it is necessary to conduct business services for the consumer, and when the receiving system's security has a similar level of protection as the sending system.

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

a. It should only be considered impossible or beyond a reasonable effort when the data is retired from further use and deleted, or retired from further use and scrambled.

8. Definitions and Categories

a. Personal Information should be defined as anything that could not be applied to other people. Every human breathes, but it is Personal Information if I use a machine to help me breathe.

b. Sensitive information

c. Deidentified should only be used to describe data that cannot be related to other data. Unique identifier should be anything I can use to locate something in a pool of information, and can be anything that requires money or identification (telephone number, billing statement number, ID number)

d. "designated methods for submitting requests" should be defined as any honest outreach in an attempt to limit data, whether it is email, phone, text, or social media contact.

e. Businesses should only be allowed to combine data from different sources when the data is not purchase, and when it was not obtained from a leaked source (originally stolen and made public)

f. .

g. "Precise geolocation" should include IP address, radio-frequency identification, GPS location, and Near-Frequency Scanning identification

h. .

i. "law enforcement agency-approved investigation" should be defined as only law enforcement trained to handle data and systems.

j. "Dark patterns" should include actions undertaken by employees in foreign jurisdictions who may not be directly subject to CCPR regulations.

Companies with foreign entities that can reach into US data systems should be scrutizined. Back-door access to operating systems should also be taken to violate CCPA under the spirit of the law by circumventing consumer's awareness of data collections.

Thank you,

Michael Weed | Workforce Management

FOREVER 21

Contact Information	US Postal /Priority Shipping
[redacted]	Forever 21 Headquarters 3880 N. Mission Road Los Angeles, CA 90031

FOREVER21.COM | FACEBOOK.COM/FOREVER21 | TWITTER.COM/FOREVER21 | BLOG.FOREVER21.COM

From: Megan [redacted]
Sent: 10/12/2021 9:52:12 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: white paper 4.18.18.pdf

[EXTERNAL]: [redacted]

See attached article on privacy audits, published at Standord CIS,
https://cyberlaw.stanford.edu/blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders

--

Megan Gray
Washington, DC
[redacted]
T: [redacted]
CV: [redacted]

Understanding and Improving Privacy "Audits" under FTC Orders

April 2018

by Megan Gray

Table of Contents

Understanding and Improving Privacy "Audits" under FTC Orders

April 2018

by Megan Gray*

I. Introduction

The Federal Trade Commission (FTC) is the primary federal agency protecting consumer privacy. The agency regularly touts its important and extensive work as the chief consumer privacy "cop on the beat." But this chest-thumping can backfire -- consumers may more readily share personal information via online platforms based on a belief that the FTC is guarding against misuse. The FTC actually has pursued only a small number of privacy cases relating to a company's unreasonable or excessive collection, use, and retention of consumer data, carving out those instances when the company acts contrary to an express privacy statement, fails to adequately protect against malicious and unknown hackers, or violates a specific federal statute (e.g., COPPA, FCRA).

This is why the FTC's 2011 and 2012 orders against Google and Facebook were heralded so heartily. For the first time, it was thought, the FTC had the unambiguous ability to ensure the companies instituted reasonable privacy protections.[1] As Berin Szoka of Tech Freedom noted, "the FTC is finding a way to regulate online privacy sans national legislation directly addressing the issue."[2] Moreover, the orders required independent,

---

* The author is a non-residential Fellow at Stanford Law School's Center for Internet and Society. This is a paper in progress, published to stimulate discussion and critical comment. The author has researched and written this paper, based on publicly available documents, in her non-work, non-family time, which is necessarily limited; she anticipates future edits will greatly improve on this draft. The views expressed in this paper are those of the author and do not necessarily reflect the author's past, present, or future employers or clients.

[1] The orders state the company must "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information..."

[2] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/.

third-party audits, it was thought, to verify the companies' compliance, thereby relieving any concern the FTC did not have the resources to monitor compliance.[3]

David Vladeck, the then-Director of the FTC's Consumer Protection Bureau, asserted, "I think the [audit] commitment that Google and Facebook have made is really an important one. Auditors are going to come in and make sure they are actually meeting the commitments laid out in their privacy policy. The audits are designed to make sure that companies bake privacy in at every step of offering a product or service. This is going to require the expenditure of a lot of money and a lot of time for companies that did not start out doing things this way. ....They've got to go back and rebuild their business in a way that takes privacy into account."[4]

According to Maneesha Mithal, of the FTC's Privacy and Identity Protection Division, "The main difference is that a [data breach] security audit is about how to protect info from unauthorized access, while a privacy audit is about how to protect info from authorized *and* unauthorized access."[5] An outside privacy expert elaborated: "[D]ata security audits...focus on ensuring that information the company has on us isn't vulnerable to hackers. But a privacy audit focuses more on how a company is using

---

[3] Not all FTC privacy or data security cases have a third-party audit provision. *See,* e.g., *FTC v. Frostwire, LLC* (2011), https://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon.

[4] "The FTC Privacy Cop Cracks Down" by Technology Review (June 26, 2012), https://www.technologyreview.com/s/428342/the-ftcs-privacy-cop-cracks-down/. *See also* David Vladeck closing letter to Google on the StreetView wi-fi collection: "...Google should develop and implement reasonable procedures, including collecting information only to the extent necessary to fulfill a business purpose, disposing of the information no longer necessary to accomplish that purpose, and maintaining the privacy and security of information collected and stored." https://www.ftc.gov/enforcement/cases-proceedings/closing-letters/google-inquiry.

[5] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/. *See also* 2012 FTC letter to Commenter Meg Roggensack of Human Rights First: "[T]he order requires Facebook to...obtain biennial privacy audits by an independent third-party professional. We believe that the biennial privacy assessments will provide an effective means to monitor Facebook's compliance with the order, including with respect to its relationship with its service providers. Each assessment will involve a detailed, written evaluation of Facebook's privacy practices over a two-year period, and will require the auditor to certify that Facebook's privacy controls have adequately protected the privacy of 'covered information' throughout the relevant two-year period." https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmbltrs.pdf.

someone's personal information internally -- how it's aggregated or re-purposed -- and when it's being shared with third parties (such as advertisers)."[6] Jim Kohm, of the FTC's Enforcement Division, predicted that any audit might take an entire six months to conduct, and would likely cost hundreds of thousands of dollars.[7]

II. Closer Inspection of FTC Privacy Orders

The initial excitment eventually dissipated. On closer inspection, the orders arguably did not require "reasonable privacy protections." Rather, the orders were more constrained, and required only a "comprehensive privacy program" that was "reasonably designed" to "address" "privacy risks." Under this language, given the companies' lengthy privacy policies essentially stating that users did not have any privacy, the FTC could face an uphill battle in asserting misuse of consumer data. This struggle would be complicated by the orders' inclusion of a reasonableness standard – the FTC carries the burden of proof in any judicial proceeding, and (arguably) no consensus exists on reasonableness in this context. Moreover, in transforming any privacy case against the companies from a Section 5-based violation into an order-based violation, the FTC arguably increased its challenges, because it would have to relinquish control over any such case -- the Department of Justice (DOJ), not the FTC, litigates the agency's civil penalty cases.[8]

---

[6] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/.

[7] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/.

[8] 15 U.S.C. §56(a) (1). If DOJ rejects the case or does not file the civil penalty action within 45 days, the FTC can file the lawsuit itself, but DOJ rarely declines FTC referrals. Few practitioners understand the legal intricacies distinguishing an FTC civil penalty case, an FTC contempt case, and an FTC Section 5 case (which itself can be subdivided into Section 5 administrative cases and Section 5 federal court cases). Key points: (a) violation of an FTC administrative order (e.g., Google, Facebook) is a civil penalty case, filed by DOJ in the name of the United States; it carries a "preponderance of evidence" standard of proof and can result in money fines without evidence of actual consumer harm, as well as injunctive relief; (b) violation of an FTC federal court order (e.g., Wyndam) is a contempt action filed by the FTC; it carries a higher "clear and convincing" standard of proof, and monetary awards are difficult to obtain in the privacy context; (c) Section 5 privacy cases carry a "preponderance of evidence" standard of proof, but, when the consumer has incurred no direct out-of-pocket loss, the company almost never pays money; and (d) Section 5 administrative cases cannot result in a monetary award, but, following the conclusion of the case, the FTC can file a second case in federal court under Section 19 to obtain financial resitution for consumers.

As a result, the third-party audits took on added significance. Because the public versions of those audits are heavily redacted and written in almost impenetrable language, the public learned little.[9] Careful review, however, shows the audits are woefully inadequate."[10]

III. Closer Inspection of Privacy "Audits" Under FTC Orders

The third-party "audits" required under FTC orders sound more impressive than they actually are.[11] For example, the Google audits evaluate just seven points, so vague or duplicative as to be meaningless. In sum: (1) Google has a written, comprehensive privacy program; (2) Google has specific employees working on the privacy program; (3) Google has a privacy risk assessment process and undertakes to mitigate those risks; (4) Google has procedures to address identified privacy risks; (5) Google monitors the effectiveness of its privacy program; (6) Google has contracts with third parties who are capable of protecting privacy; and (7) Google evaluates and adjusts its privacy program as needed when its business changes.

---

[9] Redacted versions are available on ftc.gov and epic.org. Standard FTC order language can confuse. FTC orders require an initial compliance report, which is written by the company itself and is fully available to the public (i.e., unredacted). The initial third-party "assessment" is submitted later, with only a redacted version publicly released; subsequent third-party assessments, depending on particular order requirements, might not be submitted to the FTC at all. *See*, e.g., https://epic.org/privacy/ftc/googlebuzz/FTC-Initial-Assessment-09-26-12.pdf, https://epic.org/foia/FTC/facebook/EPIC-14-04-26-FTC-FOIA-20130612-Production-2.pdf, https://epic.org/foia/FTC/facebook/EPIC-13-04-26-FTC-FOIA-20130612-Production-1.pdf, https://www.ftc.gov/system/files/documents/foia_requests/1209googleprivacy.pdf. The initial third-party Google privacy assessment, as posted at epic.org, appears to be missing page
24 but is available at ftc.gov (with the entire page redacted).

[10] *See* "Assessing the FTC's Privacy Assessments, by Chris Hoofnagle (2016), https://ieeexplore.ieee.org/document/7448350/. *See also* Robert Gellman's critique of the audits conducted by the self-regulatory organization Network Advertising Initiative (NAI): "Lacking in Facts, Independence, and Credibility:
The 2011 NAI Annual Compliance Report" (July 2012), https://bobgellman.com/rg-docs/RG-NAI-2011.pdf.

[11] "Why Facebook's 2011 Promises Haven't Protected Users," Wired (April 11, 2018) (discussing third-party audits), https://www.wired.com/story/why-facebooks-2011-promises-havent-protected-users/.

This seven-point privacy program was "audited" by an independent, third-party "assessor," whose role was merely to find some evidence that supported actual implementation of the seven points. For example, the auditor confirmed that Google has a publicly available, written privacy policy; employees who focus on privacy risks; privacy training for some employees; privacy settings available for users; a form for managers to complete when a privacy issue arises; and contractual privacy provisions with third parties.[12]

These assessments could not be more starkly different from what FTC management described in earlier news reports.[13] What happened?

---

[12] Some businesses, particularly small start-ups, may only need a de minimus privacy program like this. *See* AICPA's Privacy Maturity Model, https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf. While FTC orders require assessors to "explain how the privacy controls are appropriate to the respondent's size and complexity, the nature and scope of the company's activities, and the sensitivity of the covered info," assessors do not appear to do so, other than to verbatim parrot that text. For example, in answering this question, the Facebook assessor intones, "Based on the size and complexity of the organization, the nature and scope of Facebook's activities, and the sensitivity of the covered information (as defined in by [sic] the order), Facebook management developed the company-specific criteria (assertions) detailed on pages 77-78 as the basis for its Privacy Program. The management assertions and the related control activities are intended to be implemented to address the risks identified by Facebook's privacy risk assessment."

[13] "We don't want [an auditor] who is going to just rubber stamp their procedures," said the FTC's Jim Kohm. "So What Are These Privacy Audits That Company and Facebook Have To Do For The Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/. While the agency may not have fully appreciated this rubber-stamp risk when the orders issued, it became aware of the problem at some later point. *See,* e.g., World Privacy Forum comment in *FTC v. Uber* (September 2017), "While this requirement for assessments appears impressive on the surface, it has serious shortcomings. The obligation for an assessment is less than meets the eye.... Commission staff also sometimes refers to the assessments as audits.... We find this to be significantly misleading. We suggest that any Commission staff member who discusses a Commission consent decree in public and who refers to an assessment as an audit be required to stay after work and write 100 times '*An assessment is not an audit*'....", https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141341.pdf.

IV. An "Attestation" Is a Type of "Audit," Which Is a Type of "Assessment" that Relies on "Assertions"

Of the many audit models available from national and international standard-setting bodies, Google and Facebook selected the "attestation" model, which relies on conclusory hearsay, formally known as "management assertions."[14] As a result, assessments can be circular (e.g., "Management asserts it has a reasonable privacy program. Based on management's assertion, we certify that the company has a reasonable privacy program.").[15] The FTC's privacy cases have not usually stemmed from intentional transgressions; rather, the cases usually arise from issues the company

---

[14] The contracts ("engagement letters") between the assessors and the assessed companies are not publicly available. *U.S. v. Consumer Portfolio Services* (a 2014 FTC civil penalty case) could provide model language: "The management letter between [the company] and the third party monitor shall grant Commission staff access to the third party monitor's staff, work papers, and other materials prepared in the course of the...audit...", https://www.ftc.gov/enforcement/cases-proceedings/112-3010/consumer-portfolio-services-inc.

Because the engagement letters are non-public, and because of the heavy redactions in the assessments themselves, one cannot be sure which auditing standards apply. The assessors may not have followed the professional standards by which they are bound. The assessments state they are attestation models governed by AICPA (American Institute of Certified Public Accountants) and IAASB (International Auditing and Assurance Standards Board). AICPA categorizes privacy audits as either attestation engagements, privacy review engagements, or agreed-upon (specified auditing) procedure engagements. AICPA further subdivides attestation engagements into SOC1, SOC2, and SOC3. Based on features of the redacted Google and Facebook assessments, they are likely SOC2 attestations. AICPA subdivides SOC2 into Type 1 and Type 2 engagements. AICPA's SOC2 Guide is only available for purchase. This Guide is an authoritative AICPA interpretation and application of AT Section 101, which is the official standard for a SOC2 engagement. SOC reports are a new development, following the auditing world's transition in June 2011 from SAS 70 (AICPA's Standards on Auditing Statements) to SSAE 16 (AICPA's Standards on Attestation Engagements), a transition to align more closely to IAASB (and its ISAE 3402, which incorporates ISAE 3000 as foundation).

[15] For example, the Google assessors use the following certification language: "In our opinion, Google's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period, in all material respects...based upon the Google Privacy Program set forth in Attachment A of Management's Assertion in Exhibit I." (emphasis added).

overlooked or did not adequately disclose to consumers. A privacy audit that relies on management assertions will rarely uncover these blind spots.[16]

In a similar assessment context, one security expert opined that the attestation certification is not a seal of approval because the standard allows the company itself to decide what risks to document and what risk-management processes to adopt. "In sporting metaphor, [the company] **gets to design their own high-jump bar, document how tall it is and what it is made of, how they intend to jump over it and then they jump over it. The certification agency simply attests that they have successfully performed a high-jump over a bar of their own design."** (emphasis added). He added: "What would be really interesting would be if the company publishes their security requirements, their standards, their policies and risk assessments, so everyone can see what kind of high-jump they have just performed -- how high, how hard, and landing upon what kind of mat? It would be that which would inform me of how far I would trust a company with sensitive data..."[17]

Another security expert elaborated: "An example illustrating the difference between assessing security and auditing security might help clarify this point. Let's look at access controls. One component of access control security is a strong password policy. An assessment would check to see if the organization has a strong password policy while a security audit would actually attempt to set up access with a weak password to see if the control actually has been implemented and works as defined in the policy."[18]

Similarly, a ComputerWorld article trivialized an Uber privacy audit.[19] The article quotes from the purported audit: "While it was not in the scope of our review to perform a technical audit of Uber's data security controls, based on our review of data security policies and interviews with employees, we found that Uber has put in place and continues to develop a data seurity program that is reasonably designed to protect

---

[16] Arguably, a privacy audit relying on management assertions is wholly unsuitable when the company has been recently fined by a government agency for being less than forthright during an investigation into the company's privacy practices. In 2012, the Federal Communications Commission (FCC) fined Google on this basis in connection with its StreetView program. https://apps.fcc.gov/edocs_public/attachmatch/DA-12-592A1_Rcd.pdf.

[17] https://www.dogsbodytechnology.com/blog/iso27001-certification/.

[18] http://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm.

[19] http://www.computerworld.com/article/2880596/uber-shows-how-not-to-do-a-privacy-report.html.

Consumer Data from unauthorized access, use, disclosure, or loss."[20] The article made this point: "Let's zero in on the key utterance: 'it was not in the scope of our review to perform a technical audit of Uber's data security controls.' Based on the report and its stated methodology, the investigators weren't trying to see if Uber really obeyed its own written privacy policies. It was merely allowed to see if that written policy was an appropriate policy. But privacy policies, written by lawyers and HR specialists, are rarely the problem. The problem tends to be what employees actually do."[21]

V. Avenues to Improve FTC Privacy Assessments

The FTC's third-party privacy assessments have the potential to be an incredibly important component of the agency's enforcement program, especially given the Commission's small size and budget. The FTC, if so inclined, could pursue a variety of avenues to obtain better assessments. Most obvious, the FTC could state that "attestations" do not comply with an order's assessment provision. However, the term "assessment" is not well defined in the orders – and a common legal principle is that ambiguous terms are construed against the drafter. That said, this doctrine arguably would not apply in this situation (e.g., the term is not ambiguous because the standard dictionary definition should apply, not a technical certified-auditor definition).

Alternatively, the FTC could go beyond any submitted assessment, and conduct its own assessment under a diferent order provision.[22] The orders require companies to retain all materials that call into question the company's compliance with the order, as well as all materials relied on in preparing the assessment. Moreover, companies must respond to any relevant FTC inquiry within ten days.[23] Under these provisions, the FTC could obtain, for example, any assessment submitted to the company itself or other regulators,

---

[20] The redacted version of the Google assessment contains a similar disclaimer. "We are not responsible for Google's interpretation of, or compliance with, information security or privacy-related laws."

[21] Commenters to FTC privacy orders have raised these issues to the Commission, but the agency has not altered the assessment provision. *See* World Privacy Forum comment in *FTC v. Uber* (September 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141341.pdf.

[22] *But see* Dissenting Statement of Commissioner Maureen K. Ohlhausen, *FTC v. LifeLock, Inc.* (FTC should not fault a company's data security if a third-party assessor approved it), https://www.ftc.gov/public-statements/2015/12/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-ftc-v.

[23] *U.S. v. Morton Salt Co.*, 338 U.S. 632, 650 (1950).

domestic or foreign, and use that assessment to identify discrepancies or any areas for improvement.[24]

A. Improving Attestation Assessments

But even if the FTC did not want to entirely reject the submitted assessments or mount an argument against the "choice of model" (i.e., attestation), the FTC could insist companies submit revised assessments, improved in numerous ways, while still operating under the attestation framework. A properly designed attestation with sufficient granularity will look very much like an audit.

1. Examination Focus (Scope)

At the onset, an assessor determines the scope of the project. For a large company, attestation guidance seems to require a privacy assessment to be separately conducted along product lines.[25] By lumping multiple Google divisions (e.g., automonous cars, YouTube, search, email, voice-activated assistant, etc.) into a single privacy assessment, and using the same measuring stick for all, an assessment will have such a high level of abstraction (review at 10,000-foot level) that it serves no useful function. Noting that the redacted 2012 Google assessment is a mere 22 pages, one privacy professor opined, "How could such a short document account for all the company's information collection and handling activites from its multiple product lines?"[26]

---

[24] *See* the Irish Data Protection Commission's requirement that Facebook implement 45 granular privacy changes. As conveyed in the cover letter to the Facebook initial assessment, "Our privacy efforts received a substantial boost in 2011 and 2012, when the Data Protection Commissioner in Ireland [reviewed our compliance] with European data protection law. That review resulted in two comprehensive audit reports that documented Facebook's controls...and identified areas where we can continue to improve."

[25] "The scope of the engagement can cover (1) either all personal information or only certain identified types of personal information, such as customer information or employee information, and (2) all business segments and locations for the entire entity or only certain identified segments of the business (retail operations, but not manufacturing operations or only operations originating on the entity's web site or specified web domains) or geographic locations (such as only Canadian operations). In addition, the scope of the engagement generally should be consistent with the description of the entities and activities covered in the privacy policy." www.webtrust.org/download/Trust_Services_PC_10_2006.pdf.

[26] *See* "Assessing the FTC's Privacy Assessments, by Chris Hoofnagle (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2707163.

Similarly, Google and Facebook regularly acquire a large number of companies.[27] Their redacted assessments do not indicate how those acquisitions are folded into either the company's privacy program or evaluated during the assessment period.[28] Ironically, immediately after touting the wide variety of Google services, 30,000 employees, and 70 offices in 40 countries, the Google assessor claimed that user data falls into only 3 categories: log data, account data, and [redacted].

Given these odd attributes, the FTC could insist on revised assessments with more appropriate and explicit scoping parameters. *See U.S. v. Upromise* (2017 FTC civil penalty order violation case alleging, among other issues, that "Upromise obtained and submitted assessments that were impermissibly narrow in scope...").[29]

2. Protocol Issues (Selection of Controls and Criteria)

Many detailed protocols exist for evaluating privacy programs. The standard-bearer is AICPA's GAPP (for "generally accepted privacy principles"), which is comprehensive and granular, even providing extensive illustrative privacy controls).[30] The Google and

---

[27] https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Alphabet.

[28] The most recent Google assessment identifies its Motorola acquisition, but unilaterally carves out its compliance for over a year after the acquisition. Of separate interest, FTC orders have a provision requiring companies to report "any change in [the company] that may affect compliance obligations arising under this order, including but not limited to a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order..." (emphasis added). Arguably, the emphasized text requires reports on many acquisitions, particularly those implicating user data enhancement or user profile applications.

[29] https://www.ftc.gov/enforcement/cases-proceedings/102-3116-c-4351/upromise-inc.

[30] GAPP is of course different from GAAP ("generally accepted accounting principles"). *See* https://en.wikipedia.org/wiki/Generally_Accepted_Privacy_Principles; http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_Principles%20and%20Criteria.pdf. At last check, GAPP was being updated. ISACA (Information Systems Audit and Control Association) may also have a robust privacy protocol (denominated G31). Microsoft also promotes a robust, well-documented data governance program, https://download.microsoft.com/download/2/0/a/20a1529e-65cb-4266-8651-1b57b0e42daa/protecting-data-and-privacy-in-the-cloud.pdf, https://www.microsoft.com/en-us/trustcenter/about/transparency, https://www.microsoft.com/en-us/trustcenter/privacy/we-set-and-adhere-to-stringent-standards. Aprio is another entity that provides extensive auditing protocols for online businesses, https://www.aprio.com/wp-content/uploads/aprios-iso-27001-certification-program2.pdf.

Facebook assessments rejected GAPP in favor of customized checklists, which bear no resemblance to GAPP.[31]

By using tailor-made controls and criteria within an attestation framework, the Google and Facebook assessments are almost indecipherable, requiring certified-auditor knowledge.[32] The auditing profession uses dense and confusing terms, the meanings of which are often counter-intuitive or have a heightened-scrutiny illusion. For example, a company could be subject to an auditor's "examination" and "testing" of certain data – but this activity could be as simple as the auditor confirming that the company has a posted privacy policy. For example, the Google assessor states that it "independently tested each Google privacy control listed in the Management Assertion and Supporting Privacy Controls" and "[o]ur test procedures included, where appropriate, selecting samples and performing a combination of inquiry, observation, inspection, and/or examination procedures." Yet, pursuant to auditor nomenclature, the assessor's "inquiry test" could have been merely interviews of certain employees to ask rote questions repeating the management assertions. Similarly, while it may be reassuring to learn an assessor reviewed thousands of individual artifacts that were collected from dozens of company employees, in reality, this is meaningless without additional context (e.g., what is an artifact, were any duplicative or irrelevant).[33]

To better understand the protocol grounds on which the FTC could question the assessment, one must understand two key terms. "Controls" are policies and procedures that address risks associated with reporting, operations, or compliance and, when

---

[31] Confusingly, while the Google assessment claims to follow AICPA, it does not track GAPP. Rather, the assessment complies with AICPA rules for attestation engagements; it does not follow AICPA for the substantive protocol. AICPA procedural rules do not require use of the GAPP substance for controls/criteria; AICPA says use of GAPP is merely a recommendation. Thus, both use and non-use of GAPP is a "procedure and standard generally accepted in the industry," which is the applicable FTC order requirement. Similar to Google, the Facebook initial compliance report and the cover letter to its initial assessment claim it has adopted the GAPP framework as a benchmark, but that is not borne out in the mangement assertions undergirding the assessment. However, "[I]f a practitioner does not apply the attestation guidance [i.e., GAPP] included in an applicable attestation interpretation, the practitioner should be prepared to explain how he or she complied with the SSAE provisions addressed by such attestation guidance." AICPA AT Section 50 (para 6), Defining Professional Requirements in Statements on Standards for Attestation Engagements.

[32] While the FTC often hires consultants for technical issues, it has a limited budget. The agency could request assistance from its sister agency, the U.S. Governmental Accounting Office (GAO); James Dalkin is a GAO director with expertise in AICPA attestations.

[33] *See also* AICPA AU 325 (standards for defining "deficiency in internal control," "significant deficiency," and "material weakness").

operating effectively, enable an entity to meet specified "criteria." "Criteria" are the benchmarks used to measure compliance with the controls. In an attestation, company management selects the criteria. However, the standard-setting body for auditors conducting attestations states that "any relevant factors [that are] omitted [can not] alter the conclusion [of the report]."[34] The FTC could point to a plethora of missing, conclusion-altering factors that make the selected controls and/or criteria inadequate, as detailed below.

i. Failure to Assess Fair Information Principles: The FTC could insist the protocol include the long-standing Fair Information Principles (FIPs) -- Notice, Choice/consent, Access/participation, Integrity/security, Enforcement/redress, Use Limitation/deletion.[35] The 2012 White House's Consumer Privacy Bill of Rights also included Respect for Context, Focused Collection, and other elements.[36] An assessor who excludes a FIP from the protocol should expressly justify its exclusion. Some audits assert, "The scope of the engagement should cover all of the activities in the information cycle for relevant personal information. These should include collection, use, retention, disclosure, disposal, or anonymization. Defining a business segment that does not include this entire cycle could be misleading to the user of the practitioner's report."[37]

---

[34] *See* AT 101.24. For example, when parsed, the Google assessment shows that its management, not its auditor, determined the criteria ("PWC used pre-defined materiality criteria developed during the planning phase"). *See also* ISAE 3000, another pertinent auditing standard: "If criteria are specifically designed for the purpose of preparing the subject matter information in the particular circumstances of the engagement, they are not suitable if they result in subject matter information or an assurance report that is misleading to the intended users. It is desirable in such cases for the intended users or the engaging party to acknowledge that specifically developed criteria are suitable for the intended users' purposes. The absence of such an acknowledgement may affect what is to be done to assess the suitability of the applicable criteria, and the information provided about the criteria in the assurance report." https://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga. When last reviewed, ISAE 3000 was being finalized, and PriceWaterhouseCoopers submitted comments to weaken this portion.

[35] "Fair Information Practices: A Basic History," Bob Gellman, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020. *See also* the 2017 privacy advocates' letter to FTC commissioners on incorporating FIPs into the agency's privacy work, https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf.

[36] *See* https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b.

[37] *See* www.webtrust.org/download/Trust_Services_PC_10_2006.pdf.

ii. Failure to Map Data Flow of Consumer Information: Data flow maps are usually the key aspect of privacy audits.[38] "Understanding the data associated with personal information is useful for identifying the processes that involve or could involve personal data, and for the owner of those processes. By identifying the processes and business owners of personal information, the business can then understand the end-to-end flow of personal information including:

- Definition of specific personal information about customers and employees the organization collects and retains, including the methods in which this information is obtained, captured, stored, and transmitted.
- Definition of specific personal information that is used in carrying out business, for example, in sales, marketing, fundraising, and customer relations, including the methods in which this information is obtained, captured, stored, and transmitted.
- Definition of specific personal information that is obtained from, or disclosed to, affiliates or third parties, for example, in payroll outsourcing, including the methods in which this information is obtained, captured, stored, and transmitted.
- Identification of infrastructure components used in the receipt, processing, recording, reporting, and communication of personal information.
- Identification of personnel (including third parties) that have been granted access or potentially could access the personal information and how."[39]

From the redacted assessments, it appears companies do not map their internal or external data flows of consumers' personal information, and therefore are unable to assess whether such data goes astray. Without this, it's practically impossible to evaluate compliance with any standard.

iii. Failure to Determine Notice and Consent: Privacy policies are ubiquitous. Lesser known is that the FTC does not require such policies. Instead, the FTC mainstay is "notice and consent," and simply posting a privacy policy does not neccessarily satisfy this standard. Arguably, if a company knows or should know its consumers do not understand, and therefore cannot consent to, data collection, sharing, or

---

[38] *See* Keith Enright (now Google's Privacy Legal Director), "Privacy Audit Checklist," https://cyber.harvard.edu/ecommerce/privacyaudit.html. Mitre also provides an example of data mapping in privacy audits, https://www.mitre.org/publications/technical-papers/how-to-conduct-a-privacy-audit. It is difficult to imagine that any privacy program could effectively function without the company knowing what information it collects from consumers. It would be disappointing if Google or Facebook does not even internally keep an inventory of cookies or apps existing on its website. *See* University of California Berkeley Law's Web Privacy Census, with inventory of deployed cookies, https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/web-privacy-census/ (last conducted in 2012).

[39] https://www.journalofaccountancy.com/issues/2011/jul/20103191.html.

retention, the company has not satisfied its obligations to provide notice or obtain consent. As alleged in the *U.S. v. Upromise* complaint for violating a FTC privacy order, "...Upromise disclosed this information in such a way that many consumers would either not notice or not understand Upromise's explanation of the ... toolbar's data collection and use."[40] The assessments do not appear to evaluate whether consumers had actual notice or effectively consented to the companies' data pratices.

iv. Failure to Identify Privacy Promises: Large online companies regularly assure consumers (and regulators) that privacy is the core of their business. Such statements are frequently specific and issued at the highest level. For example, Google has a YouTube channel dedicated to privacy.[41] Yet, these company privacy statements do not appear to be inventoried or reviewed, apart from the company's essentially static, official privacy policy. The redacted assessments do not appear to identify or evaluate adherence to these more peripheral privacy statements.

v. Failure to Analyze Order Violations: The redacted assessments do not appear to address previously identified order violations or other breaches of self-regulatory programs that occurred or were discovered during the assessment period. For example, while the initial Google assessment covered the time period scrutinized in the FTC's Safari case, the assessement does not mention it, at least in the redacted version.

---

[40] *See also FTC v. Paypal* (Section 5 complaint for confusing privacy settings), https://www.ftc.gov/enforcement/cases-proceedings/162-3102/paypal-inc-matter. In the remedial *Upromise* order for violating the underlying privacy order, the FTC required the company to "obtain an evaluation and report from a qualified, objective, independent third-party professional specializing in website design and user experience ("evaluator")...For any disclosure or consent governed by Section I of the FTC Order, the evaluator must certify Defendant's adherence to the FTC Order's 'clearly and prominently' disclosure requirement and 'express, affirmative' consent requirement." https://www.ftc.gov/enforcement/cases-proceedings/102-3116-c-4351/upromise-inc. *See also FTC. v. Special Data Processing Corp.* (2004 order describing independent, third-party verification of consumer telephonic consents), https://www.ftc.gov/enforcement/cases-proceedings/002-3213/special-data-processing-corporation. In 2014, the National Science Foundation awarded large money grants to researchers to devise effective privacy notices, https://iapp.org/news/a/researchers-earn-grant-to-study-privacy-notices/. *See also* Lauren Willis, "The Consumer Financial Protection Bureau and the Quest for Consumer Comprehension," proposing that CFPB require firms to demonstrate that a significant proportion of their customers understand key pertinent facts about purchased financial products. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2952485.

[41] https://www.youtube.com/user/googleprivacy. *See also U.S. v. Google* (alleging Google's misrepresentations based on (a) privacy statement not part of official privacy policy; and (b) compliance statement vis-a-vis NAI's Code of Conduct), https://www.ftc.gov/enforcement/cases-proceedings/google-inc.

As cited earlier, an assessment's failure to include known (or even suspected) material deviations from management assertions can crater the assessment's worthiness.

VI. New FTC Commissioners May Revisit Privacy Assessment Requirements

The FTC will soon have an entirely new slate of commissioners. They may be amenable to a comprehensive overhaul of how the agency monitors its privacy orders.[42] For example, the commissioners could vote to issue a Policy Enforcement Statement, notifying all companies currently required to submit privacy asssessments that future assessments must have certain features or address particular subjects. The commissioners could also instruct staff to re-design the agency's model order language to explicitly require these characteristics in future orders.

More agressively, the Commission could pursue order modification.[43] The agency could also hire a consulting firm to create an auditing protocol applicable to all companies

---

[42] The prospect of massive civil penalties for administrative order violations is often overblown, and should not be presumed a strong deterrant. In the online context, a $41,484 per violation calculation may seem astronomical, but the statute and interpreting caselaw warrant caution. Under Section 15 U.S. Code § 45(*l*), administrative order violations can result in "no more than" that amount for each violation, with "[e]ach separate violation...[being] a separate offense, except that in a case of a violation through continuing failure to obey or neglect to obey [the order], each day of continuance of such failure or neglect shall be deemed a separate offense." If the order violation, for example, is a failure to require a vendor to sign a privacy pledge, that arguably is a single violation. In analyzing order violations, the first step is determining if the matter is a "continuing failure" or a discrete, affirmative violation. Depending on the answer to that question, the second step is counting either days or violations. And the final step is then calculating the suitable money amount for each day/violation. *See U.S. v. Reader's Digest Association, Inc.*, 464 F. Supp. 1037 (D. Del. 1979); *U.S. v. Alpine Indus.,* 352 F.3d 1017 (6th Cir. 2003) (FTC civil penalty calculated on per-day basis). Of note, the Supreme Court has indicated any civil penalty amount may have constitutional implications under the Eighth Amendment, because the civil penalty is paid to the government and determined by a jury. *United States v. Bajakajian*, 524 U.S. 321 (1998). The agency could be entirely precluded from seeking a civil penalty under the logic of *IntelliGender*, although its application to non-restitutionary civil penalties is questionable. *California v. IntelliGender,* 771 F.3d 1169 (9th Cir. 2014) (California Attorney General restitution claims in an unfair competition case precluded by a prior class action settlement on the same claims).

[43] The Commission can re-open proceedings on its own initiative to modify or set aside all or part of its order if it "is of the opinion that changed conditions of law and fact or the public interest" require it. 15 USC §45(b); 16 CFR §2.51(b). Under such circumstances, the Commission issues an order to show cause to all parties subject to the order, stating any proposed changes and the reasons the changes are needed. Each party must respond or object to the changes within 30 days; otherwise, the changes are made effective.

subject to privacy assessments. In 2011, for example, in connection with its plan to monitor healthcare providers' compliance with a new health privacy law (known as HIPAA), the Department of Health and Human Services (HHS) contracted with KPMG to develop audit protocols and assist with the audits.[44] Such a contract would be too expensive for the FTC, but the agency could seek a special appropriation from Congress or request Congressional approval to use civil penalty collections to fund the contract.

Less ground-breaking, FTC could send the company or its assessor an advance letter raising specific concerns or setting concrete expectations for the assessment.[45] In addition to the issues identified in this article, the new commission may find inspiration from the agency's "Start with Security" roadshows, which synthesized 10 principles from the agency's privacy work.[46] Needless to say, the Commission could also pursue

---

Parties themselves may also pursue order modification. The Commission recently approved Sears' petition to expand its order's online tracking provision, but did not require third-party assessments in the original order or its modification. *See* https://www.ftc.gov/news-events/press-releases/2018/02/ftc-approves-sears-holdings-management-corporation-petition.

[44] https://www.foley.com/hhs-initiates-pilot-audit-program-for-hipaa-compliance-11-22-2011/.

[45] The FTC could also send a "retroactive" letter. The legal doctrine of estoppel does not apply to government actions. *See* https://www.fcsl.edu/sites/fcsl.edu/files/ART%206.pdf. However, a five-year statute of limitations does apply to civil penalty actions. *U.S. v. Ancorp Nat. Servs.*, 516 F.2d, 198 (2d Cir. 1975); *see also Kokesh v. SEC*, 2017 WL 2407471 (U.S. Supreme Court, June 5, 2017). It is unclear if the clock starts when the violation occurs or when the agency learns of the violation. Thus, at least as a theoretical matter, the agency's prior acceptance of a company's assessment might not foreclose the Commission pursuing an order violation case less than five years following that assessment.

[46] *See also* the FTC's recent *Upromise* matter, requiring the FTC to pre-approve, not just the assessor, but the assessment's scope and design. https://www.ftc.gov/enforcement/cases-proceedings/102-3116-c-4351/upromise-inc. The Start (and Stick) with Security program addressed: (1) start with security; (2) control access to data sensibly; (3) require secure passwords and authentication; (4) store sensitive personal information securely and protect it during transmission; (5) segment your network and monitor who's trying to get in and out; (6) secure remote access to your network; (7) apply sound security practices when developing new products; (8) make sure your service providers implement reasonable security measures; (9) put procedures in place to keep your security current and address vulnerabilities that may arise; and (10) secure paper, physical media, and devices. https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business; https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.

rulemaking.[47] The agency previously studied the assessors themselves, although to what end is unknown.[48]

The commissioners could also pursue bigger-picture concepts for improving oversight of its privacy orders, described in more detail below.

A. Reconsider Legal Grounds for Redacting Assessments

Historically, the FTC has published compliance reports without any redactions, but published the assessments only in heavily redacted form.[49] The legal grounds for this disparity are unclear, and third parties seeking the assessments have not challenged the redactions in court. Evaluating whether assessment redactions are even permissible requires consideration of multiple statutes and rules. For example, the applicability of confidentiality rules and FOIA exemptions varies depending on whether the assessment is submitted pursuant to an administrative or court order, whether the assessment is characterized as being submitted voluntarily, etc.[50] A full analysis of this issue is beyond the purview of this article. That said, the subject is important enough to warrant brief discussion.

Evaluating whether the FTC is permitted to redact an assessment is not the end of the analysis. Assuming the agency has the authority to redact an assessment, the next question is whether the agency must do so. If not legally required to redact, the FTC should then consider whether the public would benefit from a full review of the

---

[47] The FTC already has a rule prohibiting some ad tracking - 16 CFR 14.12, enacted in 1978. *See* "It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking," by Jeffrey S. Lubbers, George Washington Law Review, Vol. 83, p. 1979, 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2560557 (finding materially longer time associated with the FTC's rulemaking under the Magnuson-Moss procedures, compared to rules enacted under the standard Administrative Procedures Act). *See also* "Performance-Based Consumer Law," by Lauren E. Willis, 82 University of Chicago Law Review 1309 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2485667.

[48] "FTC to Study Credit Card Industry Data Security Auditing," March 2016, https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing.

[49] Congress can obtain unredacted versions.

[50] Some FTC privacy orders (such as the Facebook order) do not require the company to submit its biennial assessments to the agency. Instead, the agency only requires the company to submit them "upon request." *See* FTC Operating Manual, Chapter 15 (Confidentiality and Access), https://www.ftc.gov/about-ftc/foia/foia-resources/ftc-administrative-staff-manuals.

assessment.[51] It may redound to the FTC's benefit to have public review and input on assessments, especially if the agency does not have sufficient resources or expertise to evaluate whether the assessors followed applicable auditing or technical standards.[52] Publication may also discourage over-reliance on management assertions, because that can negatively impact the auditor's reputation.

The agency should be prepared to counter an assessor's claim that applicable auditing rules require confidentiality of such reports. While an attestation-type audit may be a "restricted use" report, that does not mean the agency cannot distribute it. "Restricted use" merely means the assessor has to state in the report that it is not *intended* for distribution to nonspecified parties; the assessor is not responsible for controlling distribution. Indeed, the pertinent AICPA rule contemplates wide distribution: "In some cases, restricted-use reports filed with regulatory agencies are required to be made available to the public."[53] Similarly, while the contract between the assessor and the company can limit distribution, that contract does not bind the FTC.

B. Have Assessors Report Directly to the FTC

The agency could restructure the privacy orders so the FTC hires (and directs) the assessors, with the subject company order paying for the work. The agency may initially balk at this idea due to the Miscellaneous Receipts Act (MRA). Under the MRA,

---

[51] The assessed companies would no doubt object and could file a court action to prohibit publication. Or perhaps not; *see* FTC disclosure of very specific data security audit materials in document previously filed under seal in the *LifeLock* data security contempt case, https://www.ftc.gov/about-ftc/foia/frequently-requested-records/lifelock (FOIA Number 2016-00462, Final Response to Requester [Jeff Chester]).

[52] The Public Interest Oversight Board (PIOB) oversees IAASB member compliance with its auditing standards. AICPA does not appear to oversee its members' compliance with Professional Attestation Standards (AT Section 101), but the organization is affiliated with The Center for Audit Quality (CAQ). *See* "Comparing Ethics Codes: AICPA and IFAC," Journal of Accountancy, https://www.journalofaccountancy.com/issues/2010/oct/20103002.html. In Nov. 2011, PCAOB published inspection findings for PriceWaterhouseCoopers (the Google/Facebook assessor), listing serious problems with more than a third of the company's financial audits. "Inspectors noted numerous instances of problems with the testing and disclosures related to fair value measurements and hard-to-value financial instruments and with goodwill impairment…[S]ome audit problems [were found] in areas that aren't typically flagged with great frequency in major firm reports, like excessive reliance on management representations, entity-level controls…" (emphasis added), https://pcaobus.org/Inspections/Reports/Documents/2011_PricewaterhouseCoopers_LLP.pdf.

[53] *See* AU Section 532. AUs are the official interpretations of AICPA requirements (similar to the Notes accompanying each Federal Rule of Civil Procedure).

whenever an agency obtains funds other than through a congressional appropriation, the agency must consider whether the MRA applies to those funds. Money can be "received" for MRA purposes either directly or indirectly. However, money is not considered received *for the government* when the agency does not use the money on its own behalf.[54] While an extensive review of the MRA is beyond the ambit of this article, suffice to note the MRA does not apply when an FTC order requires a company to spend money as part of a program designed to prevent future violations or counter the effects of violations. For example, the FTC may use funds from a defendant to accomplish fencing-in or corrective relief, when that is a reasonable remedy for the violation. When such an affirmative remedy is appropriate, but the agency is concerned whether the violator will in fact accomplish the remedy, the MRA does not preclude the violator paying for the FTC or another entity to carry out the remedy.[55]

C. Identify and Support Violation Reporters

Historically, the agency has been loath to identify what sparks its privacy investigations.[56] But for internal purposes at least, the agency should track exactly how it

---

[54] When the Small Business Administration (SBA) was required by statute to perform annual assessments of certain companies, and the SBA required those companies to pay the third-party assessor, the GAO determined that the agency violated the MRA. In contrast, the FTC is not required to conduct assessments. *See* SBA's Imposition of Oversight Review Fees on PLP Lenders, B-300248 (Comp. Gen. Jan. 15, 2004). *See also* http://fcpablog.squarespace.com/blog/2014/10/1/the-much-misunderstood-miscellaneous-receipts-act-part-3.html.

[55] Although the FTC does not hire him directly, the FTC's *Herbalife* order authorizes the agency to terminate the independent compliance auditor and provides a replacement procedure. Notably, the compliance auditor in that case has to obtain advance FTC approval of his planned work and budget. If the FTC objects to the work plan or budget but the auditor does not resolve the matter to the FTC's satisfaction, the order provides a petitioning process to the court.
https://www.ftc.gov/system/files/documents/cases/160715herbalife-stip.pdf

[56] ProPublica, for example, was unable to learn what sparked the FTC's investigation into the 2012 Google/Safari matter. *See* https://www.propublica.org/article/announcing-225-million-fine-ftc-says-investigated-googles-internet-tracking. Tracking the investigative spark will likely require corresponding attention to initial investigations and corollary requirements for internal document retention. *See* https://hoofnagle.berkeley.edu/2016/06/29/70-of-security-investigations-closed/. Doing so may be challenging; some of the FTC's privacy cases aren't even labeled as such. The International Association of Privacy Professionals (IAPP)'s casebook is designed to capture all FTC privacy and data security cases, but it does not (as one example) list *U.S. v. Consumer Portfolio Services,* a 2014 FTC civil penalty case in which the order required a comprehensive "data integrity" program and used the "audit" term.
https://www.ftc.gov/news-events/press-releases/2014/05/auto-lender-will-pay-55-million-

learns of privacy violations, whether from internal forensic research, company whistleblowers, competitive tattletales, advocacy groups, journalists, etc. If, for example, the FTC's privacy cases are often a result of whistleblowers, knowledge of that fact can help the FTC develop best practices to encourage whistleblowers to come forward, either directly to the FTC or to the assessors.[57]

Indeed, the FTC could require assessors to consider credible privacy complaints. Well-informed consumer groups regularly send lengthy and detailed complaints to the FTC; perhaps assessors should be explicitly required to evaluate their merits (in addition to the FTC's evaluation).

In addition, given consumer groups' technical and time investment in drafting these complaints – particularly if the FTC's internal review identifies them as a frequent source of its cases – the agency could consider a order provision requiring the company to "promptly and thoroughly investigate any complaint received by [company] relating to compliance with this Order and to notify the complainant of the resolution of the complaint and the reason therefor," as the Commission required in the *Herbalife* multi-level marketing order.[58]

D. Create Positive Incentives for Subject Companies to Report Violations Independently of Assessments

Audit experts often point to an effective compliance program model developed by the U.S. Sentencing Commission.[59] The key attribute is an incentive to self-report violations. Currently, a company under FTC order has no incentive to report deficiencies in its privacy program. In fact, because data misuse (unlike data breaches) is often never discovered, a company actually has a disincentive to report problems. Rather than relying on an assessor's sleuthing abilities or a company's good faith, the FTC may be

---

settle-ftc-charges-it-harassed. Another complication may be that the FTC's records disposition requirements have not been updated since 2009. *See* National Archive and Records Administration (NARA) document N1-122-09-1, https://www.archives.gov/files/records-mgmt/rcs/schedules/independent-agencies/rg-0122/n1-122-09-001_sf115.pdf.

[57] "Ex-Facebook insider says covert data harvesting was routine," The Guardian (March 20, 2018) (describing his unsuccessful efforts in 2011 and 2012 to persuade senior Facebook executives to exercise contractual audit provisions on external developers siphoning consumer data, and his decision to denounce the company in a 2017 New York Times op-ed), https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

[58] https://www.ftc.gov/system/files/documents/cases/160715herbalife-stip.pdf.

[59] *See,* e.g., http://www.acc.com/legalresources/quickcounsel/eaecp.cfm.

well served by developing a program similar to that used by the U.S. Sentencing Commission.

"[W]hen the [U.S. Sentencing] Commission promulgated the organizational guidelines, it attempted to alleviate the harshest aspects by incorporating the preventive and deterrent aspects of systematic compliance programs. The Commission did this by mitigating the potential fine range if an organization can demonstrate that it had put in place an effective compliance program. This mitigating credit under the guidelines is contingent on prompt reporting to the authorities and the non-involvement of high-level personnel in the actual offense."[60] Other attributes of the mitigation program include:

- Oversight by high-level personnel
- Due care in delegating substantial discretionary authority
- Effective communication to all levels of employees
- Reasonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal
- Consistent enforcement of compliance standards including disciplinary mechanisms
- Reasonable steps to respond to and prevent further similar offenses upon detection of a violation

Devising a similar program at the FTC might not require legislative changes or rule-making.[61] In fact, the FTC has created safe harbors in other contexts, simply by issuing a Policy Enforcement Statement or including such a provision in a consent order.[62]

---

[60] https://www.ussc.gov/sites/default/files/pdf/training/organizational-guidelines/ORGOVERVIEW.pdf.

[61] *See,* e.g., FTC's Civil Penalty Leniency Program for Small Entities, https://www.ftc.gov/policy/federal-register-notices/notice-regarding-compliance-assistance-and-civil-penalty-leniency. *See also* the FTC's Funeral Rule Offender's Program (FROP). In conjunction with the National Funeral Directors Association (NFDA), the FTC created an industry self-certification and training program to increase Funeral Rule compliance. FROP offers a non-litigation alternative for correcting apparent "core" violations of the Funeral Rule. Violators may, at the Commission's discretion, be offered the choice of a conventional investigation and potential law enforcement action (resulting in a federal court order and civil penalties) or participation in FROP. Violators choosing to enroll in FROP make voluntary payments to the U.S. Treasury or state Attorney General, but those payments are usually less than what the Commission would seek as a civil penalty. NFDA attorneys then review the funeral home's practices, bring them into compliance with the Funeral Rule, and then conduct on-site training and testing. https://www.ftc.gov/reports/staff-summary-federal-trade-commission-activities-affecting-older-americans-during-1995-1996.

[62] For example, the FTC laid out its requirements for Section 5's "unfairness" grounds in its 1980 Policy Statement, https://www.ftc.gov/public-statements/1980/12/ftc-policy-

Alternatively, the FTC could more affirmatively inject a mitigation process into a company's privacy program. The Consumer Financial Protection Board (CFPB)'s 2016 data security order could provide a model. In addition to requiring a third-party audit (using the term "audit"), the order incorporates the common-sense realization that a robust audit is likely to identify some deficiencies at every company. With this in mind, the order lays out a process for the company to create a post-audit mitigation plan, which the company submits to the CFPB for approval along with the audit report.[63]

E. Require Board of Director Responsibility for Assessments

The FTC could require a company's board of directors to bear ultimate responsibility for order compliance. For example, the FTC could require a company's board of directors to review the third-party assessment and create a compliance plan.[64] Another model could be the 2002 Sarbanes-Oxley Act, which mandated certain corporate processes to ensure accurate financial reports, with extensive corporate board responsibilities for certifying those reports.[65]

---

statement-unfairness. The FTC has also rescinded its policy statements, as shown by the 2012 withdrawal of the agency's Policy Statement on Monetary Remedies in Competition Cases, https://www.ftc.gov/news-events/press-releases/2012/07/ftc-withdraws-agencys-policy-statement-monetary-remedies. *See also U.S. v. Civil Development Group*, (2010 FTC civil penalty case) (from the Statement of Chairman Robert Pitofsky and Commissioner Sheila F. Anthony: "Part V of the Order provides respondents with a limited rebuttable presumption that they have exercised good faith in complying with key injunctive provisions of the Order, if respondents show, by a preponderance of the evidence, that they have established and maintained the education and compliance program mandated by Part IV.") https://www.ftc.gov/enforcement/cases-proceedings/civic-development-group-llc-scott-pasch-david-keezer-united-states.

[63] *In Re Dwolla*, https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/. Although not a privacy case, the FTC incorporated a corrective action concept with the independent compliance audit required in the *Herbalife* order, https://www.ftc.gov/system/files/documents/cases/160715herbalife-stip.pdf.

[64] *In Re Dwolla*, CFPB's 2016 data security order, contains this requirement. https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[65] *See* https://en.wikipedia.org/wiki/ Sarbanes–Oxley_Act.

F. Clarify that Merely Obtaining an Assessment Is Not a Safe Harbor

After receiving an assessor's certification in conformance with an FTC order, a company could argue the FTC is precluded from contesting it.[66] But, while an assessor may determine that a certain issue is not a "material deficiency," the FTC may not agree. To avoid confusion and a company's unwarranted reliance on an assessment, the FTC could preemptively foreclose this issue. The FTC could also clarify whether a company can be in compliance with an order but still subject to a Section 5 case alleging violations of overlapping subject matter.

G. Fully Evaluate Privacy Order Provisions, including Assessments

The agency may benefit from a full cross-divisional review of its privacy order provisions, especially including the assessment provision.[67] Such self-reflection and critical analysis at the FTC is not unprecedented. On the competition side, the Commission was recently lauded, domestically and internationally, for its two-year evaluation of its merger remedies, identifying areas of both strengths and weaknesses.[68] However, the agency's Office of Inspector General reviewed the Bureau of Consumer

---

[66] *United States v. Am. Hosp. Supply Corp.*, 1987 WL 12205 (N.D. Ill. 1987) (defendant's notice to the FTC that it had acquired companies making prohibited products was not "exculpatory" but was considered "in mitigation" of the penalty). *But see* Dissenting Statement of Commissioner Maureen K. Ohlhausen, *FTC v. LifeLock, Inc.* (FTC should not fault a company's data security if a third-party assessor approved it), https://www.ftc.gov/public-statements/2015/12/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-ftc-v.

[67] Former Republican FTC Commissioner William Kovacic recently advocated a review of the agency's privacy compliance monitoring. "What kind of oversight did [the FTC] exercise? You have to look at that because that was a big part of your compliance mechanism. If that failed, then you have to rethink what you are doing." An FTC spokesman responded, "[T]he commission believes the privacy audits that undergird FTC consent decrees work." https://www.nationaljournal.com/s/665918/can-ftc-handle-facebooks-digital-privacy-challenge. *See also* privacy advocates' February 2017 letter to FTC commissioners, https://consumerfed.org/wp-content/uploads/2017/02/2-15-17-FTC_Letter.pdf.

[68] The 2017 Merger Remedies Taskforce reviewed Commission merger orders from 2006 through 2012, evaluating 89 merger orders affecting 400 markets, with 79 divestitures to 121 buyers. The Taskforce evaluated 50 of those orders using a case study method, interviewing and collecting data from nearly 200 businesses in a wide range of industries. The Taskforce Report included a list of improvements, and implemented them, specifically by updating the agency's Statement for Negotiating Merger Remedies. https://www.ftc.gov/news-events/blogs/competition-matters/2017/02/looking-back-again-ftc-merger-remedies.

Protection's resource allocation and achievement of mission objectives in 2015 and did not identify any issues associated with its oversight of the privacy orders.[69]

VII. Conclusion

The FTC is critically important to ensuring privacy protections for the public. To fulfill this mission, however, the agency should re-evaluate its orders' assessment provision, and ensure it is a robust compliance mechanism. Failure to do so could have unintended consequences for all consumers.

[69] https://www.ftc.gov/system/files/documents/reports/evaluation-ftc-bureau-consumer-protection-resources/2015evaluationftcbcpreport.pdf. *See also* FTC's Office of Policy Planning, "Post-Purchase Consumer Remedies: briefing book for policy review session," (1980), https://catalog.hathitrust.org/Record/000100549.

From: Don Marti [redacted]
Sent: 10/25/2021 11:22:11 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: CafeMedia_PRO_01-21.pdf

[EXTERNAL]: [redacted]

CafeMedia
1411 Broadway, 27th Floor
New York, NY 10018 USA

October 25, 2021

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

Dear Ms. Castanon:

Thank you for the opportunity to reply to the Invitation for Preliminary Comments On Proposed Rulemaking Under the California Privacy Rights Act of 2020, Proceeding No. 01-21.

CafeMedia, also operating as AdThrive, exclusively represents the advertising businesses of 310 small and mid-sized web publishers in California and thousands more around the world. In aggregate, those thousands of publishers represent the 10th largest property on the internet, according to Comscore. They range in size between 100,000 to more than 50 million monthly global pageviews. These independent publishers fill an important role on the internet by providing many kinds of free content to more than 173 million web users who visit at least once a month. As the largest ad representative of this type, we believe we have a unique position to speak for an under-represented constituency whose perspective is an important component of how to create a more fair and more private advertising ecosystem.

In order to provide adequate privacy protection for California residents, any future regulations must address not only transfers of personal information that take place in the open web advertising marketplace, but also sale and sharing of personal information that takes place in harder-to-measure locations within large social media platforms. The latter category, because it is not ordinarily visible to independent research efforts, presents a larger systemic risk to the privacy of California residents.

The invitation asks interested parties to comment on "How businesses should process consumer rights that are expressed through opt-out preference signals." (See Civil Code, §§ 1798.135 and 1798.185(a)(20).)

A common form of sale and sharing of consumer personal information is auction-based advertising that takes place entirely within an auction market hosted by a single social media company. Such an auction is carried out by software-implemented "bidders" that carry out individual advertising campaigns for different businesses.

After a consumer has opted out of the sale or sharing of their personal information, the CPRA requires that such information no longer be "sold" where "sold" is defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."

Markets are, by their nature, information transfer tools. This is just as true of markets within a social media platform as it is of any other market. When multiple advertisers participate in the same social media advertising platform, each advertiser that transfers their customer personal information into the system receives valuable consideration from the other advertisers. For example, consider a vendor of health education materials that transfers a customer list to a social media platform, and uses the customer list as an "exclusion list," to avoid showing its ads to existing customers. After the exclusion list is set up, a California consumer whose personal information is on the list opens a social media app and causes an ad auction to happen. Because the health education vendor is excluded from bidding, a seller of fraudulent medical devices wins the ad auction. Although the social media platform represented itself as a service provider to both businesses, the auction resulted in a "sale," as defined by the law, of personal information from one advertiser to the other. Similarly, a list of personal information used as a targeting list can result in information transferred from one business to another, as a price signal.

The law clearly does not exclude auction-based advertising internal to a social media platform from the scope of "sale or sharing." Future regulations should make it clear that personal information that pertains to a person who has opted out may not be transferred in such a way that it can be used in any internal auction on a social media platform, including as part of any "custom audience" or targeting list. The same regulations that apply to real-time bidding (RTB) advertising involving multiple firms on the open web must also apply to the same kinds of sale and sharing of personal information when it happens within a single platform.

We appreciate the opportunity to reply to this inquiry. CafeMedia, as an advertising service firm acting on behalf of independent publishers, believes that future privacy-preserving regulations and technologies can be designed to apply fairly and effectively to all businesses, and all uses of personal information. We would welcome any feedback on this letter and are available to answer any questions. Thank you.

Sincerely,

Paul Bannister
Chief Strategy Officer
[redacted]

Don Marti
VP, Ecosystem Innovation
[redacted]

CafeMedia
1411 Broadway, 27th Floor
New York, NY 10018 USA

October 25, 2021

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

Dear Ms. Castanon:

Thank you for the opportunity to reply to the Invitation for Preliminary Comments On Proposed Rulemaking Under the California Privacy Rights Act of 2020, Proceeding No. 01-21.

CafeMedia, also operating as AdThrive, exclusively represents the advertising businesses of 310 small and mid-sized web publishers in California and thousands more around the world. In aggregate, those thousands of publishers represent the 10th largest property on the internet, according to Comscore. They range in size between 100,000 to more than 50 million monthly global pageviews. These independent publishers fill an important role on the internet by providing many kinds of free content to more than 173 million web users who visit at least once a month. As the largest ad representative of this type, we believe we have a unique position to speak for an under-represented constituency whose perspective is an important component of how to create a more fair and more private advertising ecosystem.

In order to provide adequate privacy protection for California residents, any future regulations must address not only transfers of personal information that take place in the open web advertising marketplace, but also sale and sharing of personal information that takes place in harder-to-measure locations within large social media platforms. The latter category, because it is not ordinarily visible to independent research efforts, presents a larger systemic risk to the privacy of California residents.

The invitation asks interested parties to comment on "How businesses should process consumer rights that are expressed through opt-out preference signals." (See Civil Code, §§ 1798.135 and 1798.185(a)(20).)

A common form of sale and sharing of consumer personal information is auction-based advertising that takes place entirely within an auction market hosted by a single social media company. Such an auction is carried out by software-implemented "bidders" that carry out individual advertising campaigns for different businesses.[1]

After a consumer has opted out of the sale or sharing of their personal information, the CPRA requires that such information no longer be "sold" where "sold" is defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."

Markets are, by their nature, information transfer tools. This is just as true of markets within a social media platform as it is of any other market. When multiple advertisers participate in the same social media advertising platform, each advertiser that transfers their customer personal information into the system receives valuable consideration from the other advertisers. For example, consider a vendor of health education materials that transfers a customer list to a social media platform, and uses the customer list as an "exclusion list," to avoid showing its ads to existing customers. After the exclusion list is set up, a California consumer whose personal information is on the list opens a social media app and causes an ad auction to happen. Because the health education vendor is excluded from bidding, a seller of fraudulent medical devices wins the ad auction. Although the social media platform represented itself as a service provider to both businesses, the auction resulted in a "sale," as defined by the law, of personal information from one advertiser to the other. Similarly, a list of personal information used as a targeting list can result in information transferred from one business to another, as a price signal.

---

[1] Xinran He, Junfeng Pan, Ou Jin, Tianbing Xu, Bo Liu, Tao Xu, Yanxin Shi, Antoine Atallah, Ralf Herbrich, Stuart Bowers, and Joaquin Quiñonero Candela. 2014. Practical Lessons from Predicting Clicks on Ads at Facebook. In *Proceedings of the Eighth International Workshop on Data Mining for Online Advertising* (*ADKDD'14*). Association for Computing Machinery, New York, NY, USA, 1–9. DOI:https://doi.org/10.1145/2648584.2648589

The law clearly does not exclude auction-based advertising internal to a social media platform from the scope of “sale or sharing.” Future regulations should make it clear that personal information that pertains to a person who has opted out may not be transferred in such a way that it can be used in any internal auction on a social media platform, including as part of any “custom audience” or targeting list. The same regulations that apply to real-time bidding (RTB) advertising involving multiple firms on the open web must also apply to the same kinds of sale and sharing of personal information when it happens within a single platform.

We appreciate the opportunity to reply to this inquiry. CafeMedia, as an advertising service firm acting on behalf of independent publishers, believes that future privacy-preserving regulations and technologies can be designed to apply fairly and effectively to all businesses, and all uses of personal information. We would welcome any feedback on this letter and are available to answer any questions. Thank you.

Sincerely,

Paul Bannister
Chief Strategy Officer
[redacted]

Don Marti
VP, Ecosystem Innovation
[redacted]

From: Andrea Amico [redacted]
Sent: 11/2/2021 5:54:56 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 Comment on Proposed Rule-Making Under CPRA
Attachments: Privacy4 Cars - Comment on Proposed Rule Making Under CPRA - Nov 2021.pdf

[EXTERNAL]: [redacted]

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

Please find attached our comments.
Thank you for the opportunity

Andrea Amico
Founder & CEO, Privacy4Cars
c: [redacted]
www.privacy4cars.com

NEW--> CarLotz setting a new standard with Privacy4Cars
https://www.autosuccessonline.com/carlotz-partners-privacy4cars/
NEW--> Your Car Knows Too Much About You: A Privacy Nightmare
https://mashable.com/article/privacy-please-what-data-do-modern-cars-collect
NEW--> Driving Data Privacy for Cars
https://podcast.firewallsdontstopdragons.com/2021/09/13/driving-data-privacy-for-cars/
NEW--> Privacy4Cars launches security product to help dealers
https://issuu.com/usedcarnews/docs/used-car-news-5638/8?ff
ServNet leaders describe benefits of partnership with Privacy4Cars
https://www.autoremarketing.com/technology/servnet-leaders-describe-benefits-partnership-privacy4cars
ARA and Privacy4Cars partner to protect consumers whose vehicle is repossessed
https://www.autoremarketing.com/subprime/ara-privacy4cars-partner-protect-consumer-personal-information
National Cyber Security Alliance Exec Director says deleting data from cars is a must
https://www.autoremarketing.com/autofinjournal/podcast-national-cyber-security-alliance-trends-automotive

Leaving personal data in a car is a breach of GDPR
https://www.fleeteurope.com/en/safety/europe/interviews/leaving-personal-data-car-breach-gdpr
IAPP's Privacy Advisor: How one organization raises awareness over connected vehicle privacy
https://iapp.org/news/a/how-one-organization-raises-awareness-over-connected-vehicle-privacy-concerns/
Google Play App: https://play.google.com/store/apps/details?id=com.privacy4cars
iTunes App Store: https://itunes.apple.com/us/app/privacy4cars/id1370969499?mt=8&ign-mpt=uo%3D2
Twitter: https://twitter.com/privacy4cars

[1]

www.Privacy4Cars.com

PRO 01-21 Comment on Proposed Rule-Making Under CPRA

Submitted to: California Privacy Protection Agency (regulations@cppa.ca.gov)

November 2nd, 2021

Privacy4Cars is pleased to present this statement to the Agency with respect to your invitation for comment on "Proposed Rulemaking Under the California Privacy Rights Act of 2020."

Consumers in California are demanding to know how and where their personal information is being gathered and stored. The Agency has been diligent in focusing on the protection, transparency, and use of consumers personal data and we commend the Agency for inviting comments from the public.

I founded Privacy4Cars to provide simple and pragmatic ways for both consumers and businesses in the automotive industry to respect individual privacy. We believe Privacy4Cars is the first and only company focused on creating protections for the rapidly growing amounts of data collected by vehicles and have developed world-class expertise on the topic of privacy and security for vehicles. We have first-hand experience in the automotive ecosystem and we work with many industry players (automotive finance companies, auto insurance companies, dealerships, fleets, auto auctions, recovery agents, etc.) who are frustrated with how modern vehicles, services, and apps retain personal information and the significant risks associated if not properly protecting the data stored in vehicles and transmitted by vehicles.

[1] Our founder, Andrea Amico, has been heading the Privacy and Cybersecurity initiative at the International Automotive Remarketing Alliance (IARA, www.iara.biz), the industry association that reunites many of the leading players in the $100 billion vehicle wholesaling industry in the US and Canada, including automotive OEMs, automotive finance companies as large as captives and national blue-chip banks to smaller regional auto leasing and lending companies, most of the main auto auctions, large fleet management and fleet companies such as rentals, vehicle repossession companies, dealers, and many other service providers. At IARA, Amico spearheaded the formation of a partnership with Auto-ISAC, the Information Sharing and Analysis Center, established by the automotive industry to address cybersecurity and privacy issues.

Processing with significant risk to consumers

Privacy and security risks to consumers continue to grow as a direct result of companies in the automotive ecosystem refusing to offer consumers more granular choices for consent and control over how their data will be used. Privacy policies and terms of service agreements are written by auto manufacturers and third party service providers to give themselves ownership of personal information, often with the right to use it in perpetuity and for whatever purpose they see fit.

Vehicle manufacturers and service providers collect massive amounts of personal information through sensors in the vehicle, like precise geolocation, biometrics, detailed behavioral profiles of drivers and occupants (including minors), video and voice recordings, garage codes (associated with home addresses), and, when people sync their phones - a safety requirement in California (and in most states) to enable hands-free controls - a treasure trove of personal information is sucked out from the phones into the vehicles, including contacts, call logs, text messages, unique identifiers that make it easy to reassociate this data with specific individuals, and in recent vehicles much more, including social media account information, photos and files present on the phone, calendar entries, financial and health information, etc.

Yet, there is still no legal obligation for these organizations to honor consumer privacy and ensure the deletion of this personal information collected by the vehicles. As a result, more than 80% of used cars sold in the United States still include the personal information of previous owners, renters, or passengers. In 2018 I disclosed to the manufacturers of over 20 makes a Bluetooth security vulnerability that made it easy to expose and extract the personal information of previous owners, without their phones being synched nor without their knowledge (https://privacy4cars.com/data-in-cars/responsible-disclosure-and-p4c-bug-bounty/). This vulnerability was never patched for vehicles already manufactured, and we estimate that in the US alone there are tens of millions of vehicles that are vulnerable.

In 2019 we reached out again to the Automotive Information Sharing and Analysis center (Auto-ISAC) to warn them that after testing the connected mobile apps we realized there were many possible scenarios in which a person could generate or acquire credentials and consequently control the vehicle and do things such as tracking the whereabouts of vehicle occupants, remotely unlock and start the engine, etc. We were concerned of criminals exploiting such capabilities (made possible by the telematic units that are installed and enabled by default in most recent vehicles) but we got no response from the manufacturers. Persistently, we kept ringing the alarm with companies and even law enforcement agencies, including in California by speaking about the many crimes that can be committed by exploiting vehicle tech.

Sadly, at this very moment, there is a tragic case of spousal abuse in the Superior Court of California in the County of San Francisco (case #GCG20585872), which names a car manufacturer for allegedly refusing to remove remote access to the vehicle's information and safety systems from an abusive individual. When privacy is not protected in vehicles, as in this violent case, the implications can go well beyond data privacy and security breaches and into safety harm.

We also just learnt of yet another case in which a consumer, after selling the vehicle, realized he could still track and remotely operate the vehicle of the new owner. Fortunately in this instance the seller reported this gross invasion of privacy (and its dangerous safety implications) to a TV reporter. This

problem would have never occurred if the dealership had deleted the personal data from the traded-in vehicle (including the mobile app credentials of the old owner). Two years passed since Privacy4Cars disclosed this very scenario, yet to our knowledge no manufacturer has mandated that their partners (dealerships, auto finance companies, rental operators, etc.) must delete the personal information and credentials from all vehicles at every handoff. Not doing so puts at risk sellers and buyers of vehicles but also renters, consumers who got in a total loss accident, consumers whose vehicle is repossessed, not to mention businesses who may face lawsuits or be dragged in civil or criminal cases.

Automated Decision-Making

Even more sensitive information is collected via mobile apps and a robust ecosystem of third party data brokers who buy and sell personal data to a variety of organizations beyond the auto industry, including law enforcement and government. There is a growing breed of companies that collect and share personal data collected by cars. My company, Privacy4Cars, currently tracks more than 500 companies that have access to data collected from consumer vehicles, many of whom use this data for profiling and automated decision-making.

For example, many vehicle telematics-based services are advertised to consumers with phrases such as "drive with confidence, knowing an Emergency-Certified Advisor is ready to help no matter what happens out on the road." In reality, when consumers sign up for those safety services, they typically don't realize they are also granting companies the right to use their personal information for personal profiling, advertising, or even selling it to insurance companies and data brokers.

We think it is wrong to hold safety features hostage and extract consent from consumers to build detailed profiles that may affect anything from how much they pay for insurance, to how much their vehicle will be worth at resale, and of course make them targets for ads, just because they want to make themselves and their families safe. For instance, while collecting the detailed GPS location of a vehicle that got involved in a serious accident and sharing it with first responders and health organizations could be the difference between life and death for consumers, this same information should not be used to determine which ads should be served to the vehicle owner. We recommend this agency and the California legislature consider that consent for the collection, use, retention, and sharing of personal information that is strictly needed to enable safety features should be unbundled and require a separate explicit consent for all other uses, sharing, and retention of that same data.

Audits performed by CPPA

Nearly 99% of car rentals Privacy4Cars has ever audited contained personal info of previous customers and their passengers, including possibly minors. Despite multiple warnings from the FTC and even after all four major rental car companies were sued in California over this specific issue and at least two settled with the plaintiffs without prejudice, we still routinely observe data of California residents not being deleted after every rental, and leaving it potentially accessible to other people. More recently, we conducted "secret shopper" research at car dealerships and consumers reported to us that they could see the personal information of the previous vehicle owners and family members in vehicles for sale that they test drove at 88% of the dealerships they visited, just by test driving one or two vehicles of their choice. Even when dealerships claimed to have a policy in place to delete the data of the former owners, the mystery shoppers found personal information in 75% of their visits.

This is something the CPPA can audit through consumer reporting, as it does with current CCPA violations. Additionally, Privacy4Cars is building a feature within our mobile app to give consumers the ability to report when they discover personal information hasn't been deleted from their vehicle.

Consumers' right to delete, right to correct, and right to know

Privacy4Cars California LLC is a fully owned subsidiary of Privacy4Cars registered with the California Attorney General specifically for the purpose of acting as an agent for CCPA requests. We currently offer a free service for consumers to request companies to disclose what categories of data have been collected about them, for what purposes, whether the data was further shared with other third parties, and to exercise their right to delete.

To date, we've learned the time to respond to requests is highly variable, and has in cases exceeded the 45 days timeframe provided by the law. Additionally, companies often have automated responses that seem to ignore specific requests about vehicle data. For example, when requesting disclosure from Apple about what data they collect from consumers when they use Apple CarPlay, Apple points to their privacy dashboard, which does not have a section on Apple CarPlay at all. In fact, there aren't any specific details about Apple CarPlay in their privacy policy, so what data is collected from consumers using the product is completely opaque to them.

Despite the fact we clearly state in our requests that the consumer appointed us to act on their behalf, some companies annoyingly decide to respond to the consumer instead of us. The reason this is problematic is because it introduces significant friction in the system. The consumer gets the response, they don't expect an email like that or it may hit their spam filters, they have to forward it to us... all of this results in companies making it much more difficult for consumers to actually assert their rights. If the concern was about making sure that the request is legitimate, companies could decide to put the consumer in copy but leave the appointed processor in the loop. We think this agency should give clear guidance that companies should not be allowed to remove the appointed processor from the information flow, at least in all the many cases in which the actual detailed information of a consumer is not disclosed (we adopt the best practice that when processing a request on behalf of consumers, agents should never ask for the detailed information collected by a company about the subject of the request). We encountered this issue from a variety of companies, including from "privacy forward" companies like Apple.

Sometimes companies refuse to provide consumers critical information necessary for them to assert their rights. For instance, rental car companies make it difficult for consumers to know the Vehicle Identification Number (VIN) of the vehicles they rent. VIN numbers function as a standardized identifier across the industry. Even when rental companies are provided with clear information (name of the renter, date of the rental, stock unit number, etc.), they do not provide the VIN so that third parties who collect information from that vehicle (e.g. telematics providers, a variety of service providers, data brokers, etc.) can identify data collected by their company about that consumer in order to respect data subject requests for access or deletion.

Consumers' rights to limit the use and disclosure of sensitive personal information

In the automotive industry we often see that signing up for safety features will also result in the consumer authorizing companies to collect, use, and share their data for non-safety related purposes. For instance, if a vehicle is equipped with an e-call service, which triggers an emergency call in case of an accident, many vehicle owners will opt-in to this potentially life-saving feature. This safety service reasonably requires access to the detailed geolocation of the vehicle because it's necessary for emergency services to be able to locate and quickly reach the scene.

Unfortunately, when consumers sign up for this service, the opt-in experience for geolocation is also extended to a very broad set of other purposes, and often the applicable data retention policies have either very long terms such as 20 years or never expire. Companies should not have the right to extort blanket, broad consent from users by holding safety features and services hostage. Specifically, all access and use of personal information for purposes other than safety would need to have a separate, opt-in consent mechanism.

Additionally, many companies hide behind inaccurate claims that sensitive information, e.g. precise geolocation data, has been anonymized. In reality, anyone in possession of the data can easily re-identify consumers, as this report from VICE demonstrates. We believe CCPA should explicitly forbid companies from engaging in behavior, such as misleading claims of anonymization, that makes it harder for consumers to protect their information and assert their rights. Additionally, restrictions should be put on the sharing of categories of that that are virtually impossible to anonymize, e.g., geolocation and biometrics, unless a consumer explicitly consents to the sharing of this data with each individual third party.

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, with multiple questions related to the operation of a global "opt-out preference signal"

We hope California regulators who support a universal "do not sell" signal on browsers, will equally support similar measures for IoT devices, including vehicles. For example, it's possible for consumers to express their data sharing preferences by adding a prefix like "0S$" ("do not share or sell") to the name of their device and regulators should require companies to respect this expression as an opt-out preference signal.

Information to be provided in response to a consumer request to know

There is significant risk to personal information disclosed to third parties who claim to act on behalf of the consumer and reasonable safeguards are required. At the same time, we believe companies should not make it difficult for consumers to appoint a third party to act on their behalf to assert their rights when the purpose of those requests is supported by the law including: understanding what categories of data were collected, for what purpose, how they were used, with whom they have been further

shared/sold, and for what purpose they were shared/sold. Similarly, companies should not engage in behavior or restrictions that prevent consumers who appointed a third party to have their data deleted.

Definitions and categories, including clarification of the business purposes for which service providers and contractors may combine consumers' personal information that was obtained from different sources and regulations (if any) to further define "dark patterns" that are ineffective in securing consumers' consent

A common dark pattern in the automotive industry is the bundling of consent for safety features with non-safety related data collection and use. Safety features are often dangled in front of consumers in order to secure blanket consent for other purposes. This is dishonest, unethical, and should be illegal. Moreover, it's rare for any automotive company to disclose in their privacy policy the names of any third parties with whom consumer data is shared or sold. This makes it impossible for consumers to understand who may have access or possession of their data. At Privacy4Cars we currently track over 500 companies, from specialized vehicle tech companies (e.g. driver monitoring systems, mapping tools, driver behavioral scoring) to giant surveillance behemoths (e.g. Palantir). The lack of transparency of how data flows and exchanges many hands makes it unreasonable to expect that a California resident would be able to know where and how to place Data Subject Requests to get their data deleted and respected (Privacy4Cars currently offers a free experimental service to help consumers do exactly that).

Thank you for your consideration and please feel free to contact me if you need additional information.

Sincerely,

[redacted]
Andrea Amico
Founder and CEO
Privacy4Cars
https://privacy4cars.com
[redacted]

From: Cameron Demetre [redacted]
Sent: 11/8/2021 7:44:27 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Lia Nitake [redacted]
Subject: TechNet CPPA Comment Letter (PRO 01-21)
Attachments: TechNet Preliminary CPPA Letter.docx

[EXTERNAL]: [redacted]

Hello Debra,

Please find TechNet's attached comment letter for the CPPA's preliminary rulemaking. We appreciate the opportunity to provide public comment. Let me know if you have any questions and thank you for your time and consideration.

Kind regards,

Cameron Demetre
Executive Director | California & the Southwest
TechNet | The Voice of the Innovation Economy
(c) [redacted] | [redacted]
Twitter: @TechNetSouthwest

TECHNET
THE VOICE OF THE INNOVATION ECONOMY

TECHNET
THE VOICE OF THE INNOVATION ECONOMY

TechNet Southwest | Telephone 916.903.8070
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetUpdate

November 8, 2021

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

Re: PRELIMINARY COMMENTS ON PROPOSED RULEMAKING UNDER THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

Dear Board Members,

TechNet strongly urges the newly formed California Privacy Protection Agency to consider the following proposed industry feedback during their promulgation of rulemaking as it relates to the California Privacy Rights Act (CPRA). In response to solicitation for preliminary feedback to the California Privacy Protection Agency's eight specific issue sets, TechNet is providing feedback that will help to enhance interoperability across state lines for compliance purposes.

TechNet is the national, bipartisan network of innovation economy CEOs and senior executives. Our diverse membership includes dynamic American businesses ranging from revolutionary start-ups to some of the most recognizable companies in the world. TechNet represents over four million employees and countless customers in the fields of information technology, e-commerce, sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

1. ***Processing that Presents a Significant Risk to Consumers' Privacy or Security:***

We encourage the CPPA to be guided by two principles when developing rules for audits and risk assessments: (1) Privacy standards should be consistent across state lines, and (2) the CPRA directs the Agency to cooperate with other states to ensure a consistent application of privacy protections. 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.

There should be a consistent standard for assessing what constitutes a significant risk across state lines to allow for businesses to continue to build robust processes to protect consumers' information.

In determining what constitutes 'significant risk,' regulators should look at the security practices that companies have implemented. Almost all online businesses

(and many offline businesses) today "process personal information," so we should go beyond just checking to see whether that information is processed, and instead ask how it is processed and what steps are being taken to mitigate any risk to that information.

The scope of the risk assessment should be determined by 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.

Any processing of personal information beyond those identified above should not be included in the audit and risk assessment requirements, particularly the processing of personal information in any context for fraud prevention, anti-money laundering processes, screening, or to otherwise comply with legal obligations should be exempted from the scope of this definition/regulation. These activities protect consumers' privacy and security and should be kept confidential to prevent bad actors from gaining insight into our internal systems.

- *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."*

First and foremost, any new requirements via the rulemaking process should be risk-based and consistent with California's existing data security requirements, as established in Cal. Civ. Code. § 1798.81.5. This permits businesses to appropriately leverage existing cybersecurity parameters, and avoids contradictory requirements within California.

Businesses should be able to conduct self-audits, as 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. Notably, California law already contemplates that self-audits can be thorough and independent in the insurance context. *See* Cal. Ins. Code. § 900.3. Moreover, third-party audits are burdensome and expensive, making a mandate inappropriate as the burden and expense would be disproportionate to any downstream consumer benefit, and the result would likely be increased consumer costs.

Additionally, many businesses may also already perform certain industry standard audits and reports, and they should be able to leverage these certifications to meet the CPRA audit requirement in a manner that is less onerous than a separate third-party or internal audit. Existing certifications that are robust and rigorous include: the ISO 27000 series certification, the NIST Cybersecurity Framework, the annual Payment Card Industry merchant certification, CIS 20 Controls, Service Organization Control audits by internal and third parties, and security programs established pursuant to consent decrees with regulators such as the FCC or FTC. 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, such as those in the cloud computing space, to help meet their requirements to conduct cybersecurity audits and provide risk assessments.

- *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 processingconsumers' personal information and sensitive personal information.*

The regulations recognize that a single risk assessment may address a comparable set of processing operations and may encompass the business's privacy program as a whole. Accordingly, 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.

Moreover, 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.

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. Indeed, CPRA specifically states that the risk assessment requirement shall not "require a business to divulge trade secrets." § 1798.185(15)(B).

2. 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.

As currently defined in the CPRA, the term profiling is also quite broad. "'Profiling' means any form of automated processing of personal information ... to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." This arguably captures many low-risk activities like movie recommendations on a video streaming service.

To the extent California is seeking to promulgate regulations related to automated decision making or profiling regulations under the CPRA, it is important to tailor any requirements to address specific, known potential harms (versus general "we shouldn't trust machines" fears). The CPRA should apply a risk-based standard for automated decision making that reflects the fact that the risks, concerns, and benefits differ across different use cases. For example, the impacts of solely automated decisionmaking systems in AI translation services can differ significantly from those in self-driving cars or AI medical software. Regulations can be appropriately tailored to the risks by (1) applying only to fully automated decisions and (2) applying only to decisions that have legal or similarly significant effects.

If regulators are not thoughtful in crafting these definitions and corresponding requirements, it could shut down the use of automated and algorithmic technology in California. For example, it would be unworkable for most businesses to provide information to consumers on how and when a business's email spam filters make decisions to sort incoming messages. It would be equally unworkable for California businesses to accommodate individual consumers' requests to opt-out of having their emails sorted.

Finally, automated decisionmaking technology, like profiling should only be in scope as it relates to 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.

Any opt-out right or transparency requirement should not extend to activities relating to fraud prevention, abuse risk prevention, anti-money laundering processes, screening, or for other type of security or compliance activities.

- *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.

Again, to avoid a substantial burden on business activities, any regulation regarding when consumers should be able to access information about businesses' use of automated decisionmaking technology should be limited to high risk, final decisions that are fully automated, made by processing personally identifiable information, and produce a legal or similarly significant effect concerning a consumer.

Businesses should be able to fulfill consumer access requests by providing a general explanation of technology functionality, rather than information on specific decisions made.

In order to provide "meaningful" information about the logic involved in a decision, businesses should be permitted to provide a description of the general criteria or categories of inputs used in reaching a decision.

A more detailed description of any complex algorithms involved in automated decision making 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.

Any regulation should also ensure that businesses are protected from disclosing proprietary information, such as that which is subject to intellectual property or trade secret protection, in response to consumer access requests.

- *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.*

The CPRA expressly grants consumers the right to opt-out of the sale/sharing of their personal information and for certain uses of sensitive personal information. These rights are detailed in the CPRA. The CPRA does not expressly grant consumers the right to opt-out of automated decision-making. Indeed, the CPRA does not expressly grant any other opt-out rights than those above. The CPRA delegates rulemaking authority to the Agency to issue regulations related to detail around the opt-out rights granted. (1798.185(4).) And the CPRA delegates to the Agency rule making authority for "opt-out rights with respect to businesses' use of automated decision-making technology." (1798.185(a)(16).)

Since the CPRA does not create an express right to opt-out of automated decisionmaking technology, the opt-out rights referred to with respect to automated decision-making technology regulations can only mean the right to opt-out of such technology to the extent it implicates the opt-out rights for sales/sharing or use of sensitive personal information expressly granted by the CPRA. In other words, the Agency is charged with considering how the opt-out rights granted by the CPRA should relate to automated decision-making technology.

If the Agency were to issue regulations outside of these expressly granted areas, such regulations would be inconsistent with the authorizing statute and therefore void.

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.

At the outset, we caution the agency against using the rulemaking to substantively expand the opt-out rights in the CPRA, which should only come from the legislature. The core of California privacy law is the opt-out right, which is clearly defined in the statute and has been approved by voters. The ambiguous provision in the rules regarding opt-out rights and automated decision-making does not support the creation of new duties and rights that further expand the newly amplified opt-out right under the CPRA. Indeed, the delegation of such rulemaking authority, when the statute itself has not made the underlying policy choices, is unconstitutional. *Gerawan Farming, Inc. v. Agricultural Labor Relations BD.*, 405 P.3d 1087, 1100 (Ca. Sup. Ct. 2017). Furthermore, regulating outside of these areas would be an impermissible enlargement of the authorizing statute, and therefore outside the scope of the CPPA's authority. 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 twostep process: first the agency's regulation must be consistent with provision that authorizes it, if it is not then the regulation is void; second, the courts evaluate if the agency is operating within its scope of authority); In re McGhee, 34 Cal. App. 5th 902, 908 (2019) (finding regulations adopted by the California Department of Corrections and Rehabilitation ("CDCR") void as inconsistent with the authorizing statue Prop 57, because they denied some inmates consideration by the parole board to which they were entitled under Prop 57); Agnew v. State Bd. of Equalization, 21 Cal. 4th 310, 333 (1999) (holding that the State Board of Equalization exceeded the scope of authority when it imposed a burden on the taxpayer which was not imposed by the statutory authority); Henning v. Div. of Occupational Saf. & Health, 219 Cal. App. 3d 747, 760 (Ct. App. 1990) (holding that a regulation enacted by the Division of Occupational Safety and Health that required only some asbestos contractors to register with the division was void because the statute directed that "[n]o entity shall be exempt from registration" and the regulation thus exceeded the scope of authority and was void because "[a]dministrative regulations that alter or amend the statute or enlarge or impair its scope are void").

If the Agency chose to pursue an opt-out, it should only be required for automated decisionmaking, including profiling, when there is: (1) a decision made solely on an automated basis; and (2) that decision produces legal or similarly significant effects concerning the consumer. This aligns with the established standards used in the Virginia and Colorado laws, 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. Because "automated decisionmaking" is not defined in the CPRA, as written it is possible that all automated recommendation processes would be within scope. Business services routinely make a number of automated decisions in order to provide the services that people sign up for and oftentimes automation is the key benefit or purpose consumers are looking for. Specifically, automated recommendations enable personalization, which is the basis for a wide array of free and paid services.

In addition, there are some automated decisions, including profiling, that are essential to providing safe and appropriate experiences and should be excluded from the scope of the opt-out. Indeed, companies rely on automated decisions and profiling to maintain the safety, integrity, and security of their services.

First, regulators should not provide consumers a right to opt-out of low-risk automated decision making, as such a framework could be harmful to efficient business practices, with no meaningful benefit to consumers. For example, imagine if consumers could opt-out of a business using optical character recognition on PDF documents containing that consumer's personal information. Or, if consumers could inform companies that they don't want their personal information stored in an internal database that automatically sorts information alphabetically, but rather requires handwritten records be stored and sorted manually. Giving consumers the right to dictate how businesses use (or don't use) every day technology would place a tremendous hardship on companies.

Second, to the extent businesses are required to disclose use of automated decisionmaking technology in high-risk, final decisions (as discussed above), consumers will already have the ability to opt-out of automated decisions in those high-risk scenarios by declining to do business with the company.

Moreover, automation may be core to certain high-risk service offerings, making opt-outs infeasible. For example, an in-car safety system that automatically senses a crash and immediately connects a driver with assistance shouldn't be required to provide a consumer with some sort of manual process that conducts the same task – that would defeat the purpose of the automated service. Limiting the regulation to only those high-risk uses that have legal or similarly significant effects will help ensure that safety features in cars are not subject to unnecessary opt-out requirements.

Regulations should also clarify that any consumer opt-out requests should be directed to the deployer of the automated decisionmaking technology and that the role of developer of the technology should be limited to assisting the business with complying with opt-out requests, as needed.

To the extent covered by the definition of "automated decisionmaking" or "profiling" ultimately adopted by the regulations, 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. Failure to do so would, for example, enable bad actors from opting out of automated processes that detects and blocks their fraudulent activities, and limit companies' ability to protect customers' privacy and security.

3. Audits Performed by the Agency

The scope of any audit 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 under California APA procedures, enabling public comment, and should only be triggered by certain risk factors. In no event should they take place more than once every three years. The Agency should formulate its audits to avoid access to or collection of personal information.

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 90 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 audits 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.

Audits should be subject to the following rules:

- Limitations on CPPA audit authority that preclude it from auditing, or issuing findings relating to compliance or non-compliance with, any provisions of law.
- "Fair and equal treatment" rules for determining what companies get audited (e.g. either all similarly situated companies get audited, or CPPA holds probable cause hearing to formally find why a single company should be audited).
- Formal rules of procedure for CPPA audits, passed under California APA procedures to enable industry to comment.
- Formal separation / "clean team" rules within the CPPA that ensure that audit teams operate separately and independently of CPPA investigation & enforcement teams.
- Conflict-of-interest and recusal rules for any CPPA personnel involved in audits.
- Right for audited companies to nominate a reputable and mutually agreeable

third-party auditor to conduct the audit should it prefer to engage a third-party auditor.
- Scope-of-audit rules that limit CPPA audits to systems, processes, and staff involved in personal information processing activities specified in a notice of audit.
- Return & destruction requirements for materials obtained or reviewed by the CPPA during audit. Full access by audited companies to the audit file maintained by the CPPA.
- Express preservation of all applicable evidentiary and other privileges for companies that participate in CPPA audits.
- Express exemption from FOIA requests for any documents, Electronically Stored Information, or other materials produced to or obtained by CPPA in connection with audits.
- Resort to a party outside of CPPA for disputes that may arise during the course of an audit.
- Implementation of a notice requirement for the timing and the scope of audits.
- The audit should only cover the prior twelve months.

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

The CPRA sets out procedures for fulfilling requests for deletion and access, including appropriate authentication measures to help prevent fraud (Cal. Civ. Code § 1798.130). In setting out procedures and limitations on correction, the CPPA should adopt similar procedures to help provide both individuals and businesses with clarity through uniformity.

The right to correct can be an important tool for consumers when necessary to correct inaccurate information that may be preventing them from accessing 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 right to correct should be limited to basic factual information that is provably inaccurate. Consumers should not have right to demand revisions to opinions, observations, inferences, or conclusions, and it would violate First Amendment principles for them to have the ability to do so.

The regulations should also include provisions on verification of identity for a correction request that are similar to those of the CCPA. Businesses should be able to develop processes to verify identity in order to prevent fraud. It is essential for businesses to be able to use strong methods of authenticating consumers' identities prior to releasing or changing personal information.

- *How often, and under what circumstances, a consumer may request a correction to theirpersonal information.*

CPPA should seek to remain consistent with CCPA regulations as they pertain to the concept of "verifiable" requests and adopt similar guidelines.

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

The assessment should be tied to the nature of the information in question – the more significant the information the higher the "disproportionate effort" bar should be.

- *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.*

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.

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*

Private and public implementations of universal opt-outs can have negative spillover effects for both individual companies and the broader internet ecosystem. Because of this, the design of these mechanisms should be developed collaboratively with input from industry and other stakeholders. There are a few specific issues that need to be addressed when developing the technical specifications for the voluntary opt-out preference signal: First, 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. Therefore, consideration should be given to mitigating such anti-competitive incentives and encouraging the development of opt-out signals other than through browsers and operating systems. Second, companies honoring opt-out signals will inevitably receive competing signals (i.e. - a person opts out through a universal control but then opts in for a specific service). It will be important to provide guidance to companies about how to manage competing signals. Third, companies should have the ability to enable consumers to opt-in on an individual basis. There should be guardrails for this, but the relationship that businesses build with their customers should be preserved.

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.

The CPRA sets out the directive that the Agency consider these and other factors when setting for the regulatory requirements for the optional opt-out signal. It is critical that the agency develop the specifications in a way that meets this directive in order to ensure it is a meaningful and appropriately directed opt-out. Moreover, the standards for what constitutes an appropriate signal are developing in other states as well, with Colorado in particular set to start a rulemaking on such a signal with very similar directives for specifications that are set forth under the CPRA. It is critical that these signals develop in a meaningful way that is interoperable and aligned with other state models. The Agency should work with the Colorado regulatory authority to ensure that these standards develop in lockstep, rather than creating a system by which disparate signals meet the legal requirements of different statues.

Any specifications applying to these signals should also provide businesses with sufficient flexibility to implement the technical solutions that fit their business models. Businesses use a variety of solutions today, and the Agency should avoid mandating a specific type of solution that may thwart innovation and reduce incentives to provide consumers the full range of choices in opt-out solutions.

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

- *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.*

Many companies use information to improve the quality of service for all customers. Regulations should not allow consumers to opt-out of these beneficial uses of sensitive information, as the CPRA expressly allows businesses to use this information for operational purposes.

A business should also be deemed compliant with the CPRA's provisions regarding choice if it obtains opt-in consent to use sensitive personal information. This approach allows business to comply with other regimes, such as the GDPR and the

newly enacted privacy laws in VA and CO. It also is consistent with the aims of the CPRA, which is to provide consumers with choice and control over their data.

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

TechNet also has a series of more general comments, but believes categories should also cover processing relating to fraud prevention, anti-money laundering processes, screening, or for other type of security or compliance activities. Related to definitions:

Deidentified:

Align "deidentified" with VCDPA for clarity and implementability: a) remove the reference to inferring information; b) add a reference to devices linked to a consumer; and c) sharpen the distinction between "pseudonymized" and "deidentified" data by applying exceptions to "pseudonymized" data similar to those in VCDPA and CPA (e.g. carving pseudonymous data out from rights requests) — with the added benefit of incentivizing the use of privacy protective technologies even where deidentification may not be feasible.

Unique Identifier:
In "unique identifier," remove references to devices linked to a consumer and the list of example identifiers to a) clarify the definition and remove nested / circular references; and b) align the treatment of linked devices with VCDPA.

Sensitive Personal Information:
Update to sensitive personal information: to match the emerging state standard in existing omnibus privacy laws, we believe that the definition of sensitive personal information should be updated to hew more closely to categories featured in both states. This updated definition would still protect information that more accurately reflects the core of sensitive data, such as racial origin and geolocation, while eliminating less sensitive personal data like philosophical beliefs, trade union membership, and the content of messages that may not merit the same elevated protections. Rules and procedures: Under the CPRA, companies must provide a clear and conspicuous "Limit the Use of My Sensitive Personal Information" link on their homepage. A more flexible approach for operationalizing would allow companies to logically group this option together with other consumer rights, instead of forcing companies to find a separate space to meet this requirement under current law. Moreover, this control should not be scoped in a manner that is excessively granular. For example, companies should not need to provide controls that allow for a limitation of use for a particular piece of sensitive personal data or for a particular purpose. Overly granular controls may lead to notice fatigue and minimal privacy benefit for individuals.

Dark Pattern:
Regarding the definition of "dark pattern", it is important to note that the regulations should specify that the definition of "dark patterns" is focused on design practices that amount to consumer fraud.

Geolocation:
CPRA sets out a standard for "precise geolocation" that can be consistently engineered in statute. However, that definition should also specify that precise location information is: (1) is identifiable (aka de-identified/anonymous data is out of scope) and (2) excludes the content of communications (e.g. location that is manually typed in a post, or manually added to a post/photo should be out of scope).

9. Additional comments

The CPRA explicitly makes it clear in statute that nothing within the text "shall require a business to disclose trade secrets," and the CPPA should reiterate this through the rulemaking process. Whether through laborious and costly research, decades of experience, or a sudden burst of creativity, companies constantly develop information which can help them to perform better, faster, or at lower cost. Innovators in the digital economy invest time and resources, deploy their expertise and creative talents, and often extensive research to utilize the personal data provided to them by individuals to create data sets, build algorithms, and design new, innovative uses for that data to enhance their services, and people's experiences. Trade secrets are the direct product of a company's information, knowledge, inventiveness, and creativity which gives them a competitive edge and are valuable - while secret. State law recognizes the importance of protecting trade secrets from misappropriation through the California Uniform Trade Secrets Act, and federal law provides some form of protection through the Defend Trade Secrets Act. However, trade secret protections are dependent on the ability of the company to keep its intellectual property confidential. Companies in California should be assured that giving effect to an individual's right of access will not undermine their investments in their intellectual property. This is a reasonable, and proportionate balance between two rights - that of the individual, and that of the company.

Finally, one additional point to denote, every company regardless of the services and products they provide has employees also impacted by the regulations being considered. There is a real challenge with fitting some of this criteria within the human resources context. For example, 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. Therefore, the processing of "personal information" in the HR context should not be the subject of required annual audits or regular risk assessments. Requirements in the HR context, if any, as noted in the Proposition 24 preamble

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,"—Existing state and federal requirements which require businesses to collect and retain employment related records for a litany of compliance and reporting purposes. Additionally, "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 including to comply with state and federal laws. Accordingly, "sensitive personal information" should be excluded from regulations in the HR space. 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.

We appreciate your consideration of these critically important delineations. As privacy laws proliferate throughout the United States, it is even more critical to enhance the clarity and interoperability of laws and regulations that will allow companies to comply to the requirements set out by various locales. We believe the comments outlined above balance industry operability not only with the CPRA, but with existing omnibus privacy legislation throughout the world. If you need any further information, do not hesitate to reach out to Cameron Demetre at [redacted].

Sincerely,

[redacted]

Cameron Demetre
Executive Director, California and the Southwest
TechNet

From: Dan Frechtling [redacted]]
Sent: 11/5/2021 9:54:57 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 Comments on Proposed Rulemaking Under CPRA
Attachments: Boltive Comments on Proposed CPRA Rulemaking PRO 01-21.docx; Boltive Comments on Proposed CPRA Rulemaking 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 Ms. Castanon,

Thank you for the invitation for preliminary comments on CPRA proposed rulemaking. Please find attached our comments. We are providing the same document in both Word and PDF format for your convenience.

Please advise of any questions I may answer.

Best,
Dan

--
Dan Frechtling
CEO
Boltive
M: [redacted]
Boltive

November 5, 2021
California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

Re: PRO 01-21 PRELIMINARY COMMENT ON PROPOSED RULEMAKING UNDER THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

Dear Ms. Castanon,

Boltive, a privacy technology company doing business in California, appreciates the opportunity to comment on Proposed Rulemaking Under the California Privacy Rights Act (CPRA). We thank the California Privacy Protection Agency (CPPA) for seeking input from stakeholders in developing regulations.

Over five years, Boltive software has been used by hundreds of online companies to identify and block malicious and non-compliant advertising. We monitor 100 billion ad impressions per month. Recently, many of our clients have asked us to help them comply with data privacy regulations.

As a result, we have helped audit companies seeking to follow California Consumer Privacy Act (CCPA) terms. Our software helps them correct issues. We believe our general findings can be useful to the implementation of the CPRA.

Though the CPRA offers significant improvements beyond the CCPA, Boltive has discovered technical defects around transmitting consent to third parties engaged in cross-context behavioral advertising. This may allow unauthorized third parties to collect personal information.

To better ensure that consumers' opt-out requests are properly received, we recommend the CPPA:

- 1a. Clarify "requirements and technical specifications for an opt-out preference signal" to include prompt and accurate transmission of opt-outs to third parties engaging in cross-context behavioral advertising
- 1b. Audit companies for prompt and accurate transmission of such opt-outs
- 2a. Clarify "automated decisionmaking technology" to include cross-context behavioral advertising, and to require businesses to respond to consumer "access requests" about the third parties with whom their data has been shared
- 2b. Audit companies for compliance with consumer access requests.

Many entities regularly track consumers' activity online for cross-context behavioral advertising, also known as interest-based advertising (IBA) and retargeting. This continues today in California with and without consumer consent. We believe this should be remedied, as consumers should be able to effectively opt out of the sale of their personal information to third parties.

We recommend the following elements be included in rule-making.

1a and 1b. Clarify "requirements and technical specifications for an opt-out preference signal" to include prompt and accurate transmission of opt-outs to third parties engaging in cross-context behavioral advertising. Also, audit companies for prompt and accurate transmission of such opt-outs.

Programmatic advertising employs auctions that occur in less than 200 milliseconds. The bidder with the most personal data about the website visitor seeing the ad often wins. A single ad request splits into dozens of requests, as publishers fan out to their supply side platform (SSP) partners, SSPs forward to other SSPs and ad exchanges, and so on. The process continues to demand side partners (DSPs), who represent advertisers and agencies. Also known as real-time bidding (RTB), this has been the subject of investigations by authorities in the UK and Belgium.

Boltive has built software that looks for consent failures. We track if a consumer's "Do Not Sell" declaration is passed correctly to the above partners bidding for an ad. Companies use our software to confirm they and their partners follow privacy principles.

Strictly speaking, we are auditing some terms of the CCPA in the wild and helping clients correct issues. Across our live pilots with online companies, we see 15-20% of consent requests are failing due to technical issues. When this happens, consumers who have opted out appear to have opted in or appear ambiguous to the recipients of requests. Those consumers may be targeted and retargeted by advertisers they sought to avoid.

In addition, our data is telling us the issue has a broad footprint. We have documented more than 50 advertising vendors involved in incorrect opt-out signals. These include some of the biggest players in the online advertising industry. We believe the errors are for the most part unintentional and not deliberate.

These findings are early and will be augmented over time as we run more live trials and as we test different opt-out mechanisms, such as industry protocols (DAA, NAI), global privacy control (GPC), and others.

Clearly the intent of CPRA goes beyond advertisers and data controllers to downstream partners and data processors. But the statute is not clear in this regard. Civil Code, § 1798.185(a)(19)(A) calls for 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." But specifics are missing.

We recommend the CPPA be clear in its rule-making that the "requirements" for the "opt-out preference signal" include downstream compliance with the consumer's request. Specifically, we suggest a requirement that the *signal be authentically received by all of the successive parties in the advertising chain that must act on the signal.* Only with this clarification can consumers feel safe their opt-outs are neither lost nor misinterpreted as opt-ins.

Furthermore, we support clarifying the audit authority mentioned in Civil Code, § 1798.185(a)(18) as well. We recommend the audit scope to include verifying that opt-outs noted above are authentically passed and received by parties in the advertising chain. This oversight will have a positive influence on compliance.

Monitoring the multitude of opt-outs initiated by consumers every day may seem a tall task. Fortunately, these audits, whether performed by businesses internally or by the CPPA for enforcement, are easily accomplished with software automation that does not involve personal data and that operates in a standalone fashion, requiring no installation or integration by the CPPA.

2a. Clarify "automated decisionmaking technology" to include cross-context behavioral advertising, and to require businesses to respond to consumer "access requests" about the third parties with whom their data has been shared. Also, audit companies for compliance with consumer access requests.

We believe cross-context behavioral advertising is a form of "automated decisionmaking" mentioned in Civil Code, § 1798.185(a)(16) because programmatic advertising is automated *by definition* and these automated systems decide how to classify and target individuals. We also believe cross-context behavioral advertising is a form of "profiling" mentioned in 1798.140(z) because it is "automated processing of personal information…to evaluate certain personal aspects relating to a natural person."

When consumers make access requests about the logic involved in automated decisionmaking processes mentioned in 1798.185(a)(16), they should be entitled to know with which third parties their personal information is shared. Boltive has found the nature of third parties makes a big difference. Boltive has documented examples of foreign malware companies extracting data from the "bid stream," which represents the personal data flow of online advertising. For similar reasons, the European Data Protection Bureau (EDPB) has recommended companies map to whom personal data is transferred in the EDPB's Know Your Transfer recommendations.

Furthermore, we recommend the audit authority mentioned in Civil Code, § 1798.185(a)(18) include verifying that companies have logged and mapped the

companies with whom they share data for cross-context behavioral advertising so such information can be shared with consumers.

A counterpoint to the above recommendation is that such logging and mapping creates an unfair burden to businesses. We wish to avoid the weight of manual processes encumbering companies. Fortunately, identifying third and fourth parties can be accomplished with software automation that does not involve personal data, and that operates in a standalone fashion.

Closing

We continue to monitor and gather data around consent opt-outs and unauthorized data collectors so companies can comply with CCPA, CPRA, and industry standards such as generally accepted privacy principles (GAPP), privacy by design, and the like. Thank you for consideration of our comments. Please do not hesitate to reach out if you have any questions.

Respectfully submitted,

Dan Frechtling
CEO
Boltive

From: Recht, Philip R. [redacted]
Sent: 11/5/2021 2:49:36 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO-01-21 [MB-AME.FID3272618]
Attachments: PRO-01-21 Preliminary Comments on Proposed Rulemaking Under CPRA.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.

Philip R. Recht
Mayer Brown LLP
350 S. Grand Avenue, 25th Floor
Los Angeles, CA 90071
Direct: [redacted]
Main: 213 229-9500
Mobile: [redacted]
Fax: 213 625-0248
[redacted]

MAYER | BROWN

Mayer Brown LLP
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071-1503
United States of America

T: +1 213 229 9500
F: +1 213 625 0248

mayerbrown.com

Philip R Recht
Partner
T: [redacted]
F: +1 213 576 8140
[redacted]

November 5, 2021

BY EMAIL

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

Re: PRO-01-21: Preliminary Comments on Proposed Rulemaking Under the CPRA

To whom it may concern:

Our firm represents a coalition of companies (i.e., Spokeo, PeopleFinders, MyLife, Truthfinder, BeenVerified, and PeopleConnect) that provide background check, fraud detection, and other people search services. We appreciate the Agency's September 22, 2021 Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (CPRA) and write to address a single issue of potential rulemaking, i.e., notice at collection by businesses that collect personal information (PI) indirectly from third-party sources, rather than directly from consumers. We recommend and request that the Agency leave in place 11 Cal. Code of Regulations (CCR) section 999.305(e) (hereinafter "Regulation 999.305(e)"), which permits companies that register as data brokers to meet the notice at collection requirement by including in their registrations a link to their online privacy policies that include instructions on how consumers can submit requests to opt out.

I. Our Clients

Our clients provide background check, fraud detection, and other people search services. They do so, like others in the data industry, by collecting data mostly from publicly available sources, organizing the data into usable products (such as reports), and offering the reorganized data for sale to customers. Unlike businesses that collect personal information directly from consumers and then sell that information, our clients collect the information they sell only from third-party sources.[1]

Our clients' services are widely used and highly valued by an array of public and private entities and individuals. Law enforcement agencies use the services to identify and locate suspects and witnesses, and to serve subpoenas. Welfare agencies use the services to find parents evading child support awards. The Veterans Administration uses the services to locate next-of-kin of

[1] Our clients have direct relationships with customers, who provide PI as part of the customer relationship. The concerns raised in these comments do not apply to customers, to whom our clients can and do provide direct notice at collection.

fallen soldiers. Businesses use the services to detect order fraud and update customer and prospect databases. Consumers use the services to find lost relatives and friends, plan family reunions, check out relationship prospects and online marketplace sellers, and to root out scams.

II. Notice at Collection by Data Brokers

The California Consumer Privacy Act of 2018 (CCPA) requires that covered businesses inform consumers of certain data collection practices "at or before the point of collection." Civil Code § 1798.100(b). The current regulations refer to this notice as the "notice at collection." 11 CCR § 999.301(l).[2] The CPRA, at new Civil Code section 1798.100(a), retains this notice requirement for businesses that control the collection of consumer PI.

The giving of notice at collection is a relatively straightforward proposition for businesses that collect PI directly from consumers. Those businesses may provide the notice directly to a consumer as part of their initial transaction or interaction with the consumer. Indirect collectors, however, do not (and may never) interact with consumers directly and, thus, do not maintain direct relationships or accounts with consumers. As such, it is impossible for indirect collectors to give direct notice to consumers "at or before" the collection of the consumer's PI. At that point in time, the businesses lack any information, contact or otherwise, about a consumer. Even after indirect collection, the contact information collected from third-party and publicly available sources is often out-of-date and/or incomplete, rendering any attempts at direct notice based on such contact information ineffective, both for businesses and consumers. For example, a postcard mailed to an old address or an email sent to a defunct account provides no meaningful or effective notice.

In recognition of and to address these concerns, the Legislature and AG took complementary actions. First, the Legislature in 2019 enacted the Data Broker Registration law. Civil Code § 1798.99.80 *et seq.* That law—which our clients supported—requires data brokers[3] to list their name and primary physical, email and internet website addresses on the public AG data broker registry. Doing so ensures that consumers know both the existence of data brokers and how to contact them.

Next, the AG in 2020 promulgated Regulation 999.305(e), which provides that "[a] data broker registered with the [AG] … does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out." Other portions of the AG regulations—specifically, 11 CCR sections 999.308(c)(1)c. and g.—require online privacy policies to include the same disclosures as the notice at collection. Thus, Regulation 999.305(e)

---

[2] We previously submitted comments to the Attorney General (AG) on this and other topics on February 13, September 30, and December 6, 2019. In those comments, we referred to the notice at collection as the "pre-collection notice."

[3] A "data broker" is a business that both collects the "personal information of a consumer with whom the business does not have a direct relationship" *and* sells that PI. Civil Code § 1798.99.80(d).

ensures that data brokers availing themselves of this option not only alert consumers to the companies' operations in California, but also accomplish the notice at collection goal of informing consumers (through the companies' privacy policies) of the companies' data collection and use policies (not to mention additionally informing consumers of the means by which they may exercise their opt out rights).

The CPRA gives data brokers and other indirect (third-party) collectors a second option for providing notice at collection. Specifically, new Civil Code section 1798.100(b) provides that such businesses "may satisfy" their notice at collection obligations "by providing the required information prominently and conspicuously on the homepage of its internet website." This alternative (using the word "may") is permissive, not mandatory, in the same way that registered data brokers are given the option under Regulation 999.305(e) of including a link to their privacy policies (with opt-out instructions) to satisfy the notice at collection requirement, but are not required to do so.

We have no objection to either of these alternatives. On the contrary, we strongly recommend and request that the Agency preserve Regulation 999.305(e) in its current form when issuing new and updated regulations under the CPRA. Retaining the registry notification gives data brokers two options for communicating the notice at collection (i.e., on their homepages or on the registry, provided the registration contains a link to their privacy policies), providing valuable flexibility for complying with the laws.

Equally important, retaining Regulation 999.305(e) gives consumers multiple options for identifying data brokers and their data collection practices. A consumer that does not know the name or existence of a data broker may not find his or her way to the business's internet homepage (and any notices thereon), at least not without great effort or assistance. The data broker registry provides consumers with a single location to identify all data brokers operating in California. When data brokers include links to their privacy policies and opt-out instructions—as encouraged by Regulation 999.305(e)—the registry becomes a one-stop shop for consumers. Indeed, the data broker registry has existed since January 2020, and many data brokers have chosen to provide direct links to their privacy policies and opt-out mechanisms (*see*, e.g., https://oag.ca.gov/data-brokers). Eliminating or amending Regulation 999.305(e) likely would cause data brokers to omit such links from their registration submissions, thereby frustrating consumers who have come to rely on the additional information in the registry. Retaining Regulation 999.305(e) satisfies consumer expectations and meets the CPRA's goals of giving consumers clear, conspicuous, and actionable data privacy information and choices.

We hope these comments are helpful. Please let us know if you have any questions. If appropriate, we would welcome the opportunity to speak to you further about the issues discussed herein.

Yours sincerely,

Philip R Recht
Partner

From: Pelakova, Lenka [redacted]
Sent: 11/5/2021 1:50:59 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: CPRA_rulemaking_comments_FINAL.pdf

[EXTERNAL]: [redacted]

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

Dear Ms. Castanon,

Please find attached Avast's comments in response to the Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 published by the California Privacy Protection Agency on September 22, 2021.

If you have any questions, please do not hesitate to contact us.

Best regards,

Lenka Pelakova
Privacy Counsel
[redacted]
avast.com

Protecting digital freedom for everyone.

Avast

In Redwood City, November 5, 2021

Re: Preliminary Comments on the Proposed Rulemaking Under the California Privacy Rights Act of 2020

To Whom it May Concern,

We welcome the opportunity to provide our feedback on the proposed rulemaking under the California Privacy Rights Act of 2020 ("**CPRA**"). As a company with more than 435 million users around the world whose digital freedom we are striving to protect, we take the protection of privacy very seriously and are eager to participate in the public debate about current privacy issues, and to build collaborative and transparent relationships with the privacy and data protection authorities in all jurisdictions where we maintain presence, including in the state of California.

1. Introducing Avast

Avast is a world leader in consumer cybersecurity and privacy, protecting the digital lives and rights of millions of users and businesses worldwide. On average, our solutions block over 1.5 billion malware attacks and over 33 million phishing attacks each month on average. Headquartered in the Czech Republic, we employ over 1,700 people globally and have our largest markets in the U.S. and Canada, Brazil, France, Russia, and Germany. Our role is to make the online world a safer place so that digital citizens are free to connect and enjoy safe and private lives. With an award-winning, cross-platform portfolio of antivirus, security, privacy, and performance products, Avast is best known for keeping people safe from growing threats such as ransomware, stalkerware, spyware, Wi-Fi-based threats, IoT attacks, and browser-based risks.

Based out of the European Union ("**EU**") for over three decades, Avast has extensive experience navigating complex and sophisticated data protection laws, in particular, the EU's General Data Protection Regulation ("**GDPR**").

2. General Comments

On the overall, we welcome the fact that the California Privacy Protection Agency ("**CPPA**") is committed to implementing robust privacy protections for California residents, and we recognize that the CPRA, along with its forerunner, the California Consumer Protection Act ("**CCPA**"), represents a revolutionary shift in the U.S. legal landscape, being the most comprehensive consumer protection law in the nation. This unavoidably comes with certain challenges for both businesses and consumers alike as to the interpretation and understanding just what 'privacy compliance' looks like. It is for this reason that we find that adding clarity by way of rulemaking with an added layer of detail would contribute towards building legal certainty, consumer awareness, and meaningful and effective compliance programs for the businesses covered by this law. We also view this opportunity as very important since although California is one out of fifty U.S. states, it represents an eighth of the nation's population and roughly 14.7 % of its GDP. Coupled with California's historical - and continued - role in the development of science and technology and fostering groundbreaking innovation, we believe that the CPPA is in a unique position to set trends the rest of the union would likely follow.

We believe that the key to a successful implementation and enforcement of robust new privacy protections is to ensure that the privacy and privacy rights of consumers are strongly protected, and also that obligations are constructed and enforced in ways that are clear, workable, and effective for both businesses and the CPPA. If the

rulemaking succeeds in striking the right balance between these interests, we believe this could serve as a model for strong protections that the U.S. could later adopt more broadly.

Another point, which will become relevant in several areas discussed in more detail below, is the possibility of approaching the rulemaking in such a way that it would bring the CPRA and its associated regulations into alignment with their substantive equivalents in other regional and global standards, such as the GDPR. For instance, it would help make California-based businesses competitive on a global scale without the need to perform additional complex compliance exercises in order to introduce their products or services to the EU's massive single market. In particular, commonalities and consistency between certain elements of the CPRA rulemaking and the GDPR would ensure that California-developed products are launched with EU-friendly privacy solutions already built in, reducing the costs of EU compliance, thus lowering the barrier of entry into the EU markets. As a result, global expansion would not be limited only to those California businesses that can afford to conduct costly and time-demanding GDPR compliance projects, but it would also become an option for smaller businesses, such as startups.

More importantly, alignment between certain elements of the CPRA and the GDPR would be beneficial for the consumers as well. Some Californian consumers already do have GDPR-style privacy rights with respect to their personal information processed by businesses that are subject to the GDPR, and these consumers may have come to expect a certain level and style of privacy rights from the businesses they interact with, especially in the online space. A lack of alignment on these fundamental rights and obligations could lead to uncertainty across the California market, where one segment of consumers would expect to have GDPR-style rights while another segment may not even be aware of the fact that they have any privacy rights at all. Increasing consistency and alignment between regional and global privacy standards, such as the CPRA, the GDPR, Convention 108+, and the OECD Privacy Framework, would contribute towards increasing clarity across the board, saving consumers the time and effort it would take to research what rights they have where and under what circumstances.

These general comments aside, there are also several specific points concerning the proposed rulemaking that we would like to raise for your consideration. We elaborate on these points below.

3. Specific Comments

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

As an opening note, Avast would like to point out that the obligation to proactively submit to the CPPA regular risk assessments regarding their processing of personal information could, if not calibrated correctly, create excessive administrative burden for both businesses and the CPPA, without providing the benefits that the CPRA envisages it could provide. An overly broad, general approach could potentially create inconsistencies, where different businesses would adopt different approaches due to subjectivity of interpretation.

The need to make sure these obligations are imposed only where necessary is further compounded by the fact that conducting risk assessments meeting the high standard required for any submission to a governmental authority may prove to not only be financially costly, but also demanding in terms other than financial, *e.g.,* requiring time, money, manpower and operational bandwidth. Not every operation can afford these costs. As a result, this could lead to an effective gatekeeping of compliance, where only the big players, such as large tech companies, would be able to afford to expend the resources and services necessary to carry out these risk assessments on a business-as-usual basis, leaving start-ups, new market entrants and smaller market participants at a compliance-competitive disadvantage.

Avast is therefore of the view that to level the playing field, the legal obligation to proactively submit the risk assessments to the CPPA should only trigger as an explicit requirement with respect to those businesses that process the personal information of 10,000,000 (to wit: ten million) or more consumers in a calendar year, with it being a

recommendation of best practices with respect to the rest. This approach would also be consistent with existing California rulemaking under the CCPA and it would ensure that compliance is scalable, meaningful and effectively targets the truly problematic processing operations across the whole market.

We would also like to emphasize that this is without prejudice to the CPPA's ability to compel a business to disclose risk assessments under the administrative powers vested in it by the CPRA.

Lastly, Avast is of the view that this approach would also prevent putting unnecessary pressure on the CPPA, which would have to receive, file, review and possibly follow up on a large volume of risk assessments on an ongoing basis, leading to throttling and adversely affecting the CPPA's ability to carry out its role. As an alternative, these regular submissions could be replaced by an obligation to conduct a project-specific data protection impact assessments ("**DPIAs**") in situations when the proposed processing operation is likely to result in a high risk to rights and freedoms of consumers.

Below we provide our view on the individual questions posed by the CPPA.

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

It needs to be ensured that the "significant risk to consumers' privacy or security" is reserved for only the kind of processing that is likely to result in high risk to rights and freedoms of consumers, *i.e.,* liable to have the most significant impacts on a consumer's life. The relevant metrics could include significant harm, such as bodily harm, humiliation, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property and processing that produces legal effects or any harms relating to personal identity or informational self-determination. Furthermore, in order to add legal clarity, the CPPA rulemaking could list the types of processing operations which present significant risk to consumers privacy or security - in a similar manner to the lists of processing operations which require a DPIA set out by European data protection authorities - where these could include:

(i) Systematic and extensive profiling with significant effects;
(ii) Large-scale use of sensitive personal information;
(iii) Public monitoring;
(iv) Evaluation or scoring;
(v) Automated decision-making with legal or similar significant effect;
(vi) Systematic monitoring;
(vii) Processing of sensitive personal information or data of a highly personal nature.
(viii) Large-scale personal information processing;
(ix) Matching or combining datasets;
(x) Data concerning vulnerable consumers (*e.g.*, children, the elderly);
(xi) Innovative use or applying new technological or organizational solutions;
(xii) Preventing consumers from exercising a right or using a service or contract.

At the same time, for greater clarity, the CPPA should also define some areas that do not present a "significant risk to consumer's privacy or security", *i.e.,* are exempt from this obligation. These exemptions should cover, in particular:

(i) "Business purpose" within the meaning of the CPRA; and
(ii) "Research" within the meaning of the CPRA, especially research in the area of cybersecurity and new and emerging threats.

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."*

Requiring that cybersecurity audits be performed on an annual basis as an express obligation under the law imposes a considerable regulatory burden upon a business and can run counter to the interest of providing effective protection, *e.g.,* by diverting the limited resources a business has available. It may be helpful to allow for the demonstration and maintenance of generally recognized certifications or standards to be sufficient to indicate security maturity. SOC type 2, for example, could be recognized by the contemplated rulemaking as sufficient proof of thoroughness and independence. This would mean that those businesses that already expended considerable resources into adopting sophisticated security practices would have legal certainty about the sufficiency of their level of security, thus avoiding additional compliance work which would be unnecessary, while, at the same time, this approach would encourage those who do not have any certifications in place to obtain them.

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.*

As was mentioned above, Avast is of the view that CPRA rulemaking presents an exciting opportunity to align the California approach to privacy law with that of the EU, namely, the GDPR, thus increasing California's businesses ability to compete on a global market. To that end, we believe it is efficient to model the risk assessments after the "data protection impact assessments" established under the GDPR. As such, the CPRA risk assessments should take into account the nature, scope, context and purposes of the processing, with the minimum features of such as assessment including:

(i) a description of the envisaged processing operations and the purposes of the processing;
(ii) an assessment of the necessity and proportionality of the processing;
(iii) identification of the risks to consumers' rights and freedoms;
(iv) an assessment of the risks to the consumers' rights and freedoms; and
(v) the measures envisaged to:
    a. address the risks; and
    b. demonstrate compliance with the CPRA and its associated regulations.

At the same time, as a matter of good practice, a risk assessment should be reviewed and re-assessed on a regular basis, especially where changes are introduced into the process.

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.*

In order to assess whether the risks to the privacy of the consumer outweigh the benefits of a business processing their information, a variety of factors should be taken into account. The (non-exhaustive) list of these factors should, at minimum, include: (i) the nature of the personal information the business intends to process (*i.e.*, is it "regular" or sensitive personal information, or is it something in between?), (ii) the scope of processing and aggregation (discussed in more detail below), (iii) the reasonable expectations of consumers, (iv) the likely impact of the processing on the consumer, and (v) whether any safeguards can be put in place to mitigate the negative impacts.

The more sensitive or 'private' the information, the more closer a processing operation gets to being considered intrusive or capable of creating risks to consumers' rights and freedoms, e.g., by putting them at risk of discrimination. Conversely, where the information processed is less sensitive or 'private', then the impact would be less problematic (although this impact would need to be considered regardless).

At the same time, what needs to be taken into account in assessing risks to consumer privacy is not just the nature of a particular piece of information when taken at its face value. Information can become sensitive by association with (links to) other information, creating information that is sensitive because it was put in context or aggregated, even if it would not fall into that category on its own. Therefore, aggregation of personal information should be a factor that contributes towards raising the level of risk to consumers' privacy or security and the assessment should take that into account.

(ii) Automated Decisionmaking

Without fully-fledged regulation in the area of artificial intelligence ("**AI**"), one way in which responsible and ethical use of AI can be established in law is through privacy laws. Although imperfect, the GDPR represents a good example of how privacy or data protection regulation can be used to provide basic protections to the rights of individuals in the AI context.

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

First of all, it is important that the CPRA rulemaking covers all possible mechanisms of profiling, in particular: (1) general profiling, (2) decision-making based on profiling; and (3) solely automated decision-making that includes profiling. More specific examples of profiling could include:

(i) procedures involving statistical deductions used to make predictions about people (predictive analysis);
(ii) assessments of a consumer's ability to perform a certain task;
(iii) assessments of a consumer's interests or belief systems;
(iv) assessments of a consumer's likely behavior; or
(v) evaluation of a consumer in the context of a contract (*e.g.,* evaluation carried out by a bank in deciding whether to provide the consumer with a loan or mortgage and if so, on what terms, evaluation carried out by a car insurance provider whether or not to alter the insurance fee paid by the consumer based on the consumer's driving habits, *etc.*).

We also understand that the similarities between the terms 'profiling' and 'automated decision making', especially in an era of widespread and rapid technological advancement, could lead to some legal certainty, as the issue is complex. Automated decisions can be made with or without profiling. It is therefore important that the CPPA rulemaking addresses this issue and offers guidance as to the relationship and scope of these two terms.

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

We believe there should be full transparency in processing of personal information that leverages the use of automated decisionmaking technology. The process to facilitate consumer access to information should be user-friendly, easy to locate and readily available. In particular, the CPPA should specify that "burying" the mechanism through which consumers can exercise their rights under layers of menus, options or labyrinthine website structures would not be considered CPRA compliant.

We believe that all consumer rights under the CPRA should be exercised by the consumer freely, while fully informed, and with as few limits as possible. The information about a business' use of automated decisionmaking technology should also be included in its general privacy notice under the CPRA, including the meaningful information about the logic involved.

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.*

Use of personal information for AI processing, including automated decisionmaking, should always be transparent. A general right of access should include meaningful information about the logic involved. In order for this information to be meaningful, it should not utilize technical or legalistic terms, nor should it be overly complex. For the information to be "meaningful", it needs to explain the underlying logic in plain and simple English (*e.g.,* by way of "if – then" statements) and the general role and the lifecycle of a consumer's personal information within that logic. Where the processing involves scoring or ranking, this information should also include the explanation as to the underlying logic of such scoring or ranking, *e.g.,* what are the factors that are relevant for the score or rank.

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

Consumers should have the right to object to (opt out of) decisions concerning them which produce legal effects or similarly significant effects based solely on automated processing, including profiling, unless it is necessary for entering into, or performance of, a contract between the consumer and the business, or is authorised by law, and in both cases only where suitable measures to safeguard the consumer's rights and freedoms and legitimate interests are in place, such as the right to obtain human intervention, to express their point of view, and to contest the decision.

(iii) Consumers' Rights

As regards consumers' rights, Avast would like to reiterate that, as mentioned above, Avast is of the view that California would benefit greatly from CPRA regulations that would align with the approach under the GDPR, in both content and practice. Responding to consumer requests is a large-volume, technically and operationally challenging process. Larger companies would have GDPR-style systems in place, but for smaller companies seeking to expand outside of the US, it would be quite challenging to adapt its compliance programs to different regulatory standards. Creating new, similarly-named but different sets of obligations from international and regional standards, such as the GDPR, would result in a situation where the differences in similar-sounding rights would be so tricky and difficult to navigate that only those market players who could afford to analyze and do the additional compliance work would be allowed to expand to markets beyond California or the US. Therefore, we are of the view that bringing the CPRA rulemaking and practice closer to the GDPR would contribute towards California businesses of all sizes to be truly competitive on the global market.

Furthermore, as was mentioned above, aligning the approach to consumers rights with the GDPR would also be beneficial to consumers – adding more clarity as to what they are entitled to under the law, providing consistently robust safeguards to their rights and creating a more privacy-aware, rights-savvy consumer base.

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.*

On top of the existing construction of the right to correction, we believe that as the use of AI technologies, in particular, for automated decisionmaking, becomes more widespread, the right to correction should extend to the use of such technologies. In particular, we believe that the right to correction should not apply to not only input data, but also to output data. In other words, the consumer should have the right to remedy the results of an automated process made on the basis of that consumer's personal information.

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

We are of the view that the consumer should not be unduly limited in exercising their rights, including the right to correction, and that there should be as few limitations as possible. At the same time, a business should be able to refuse acting on a consumer request if that request is manifestly unfounded or designed to be disruptive. The business should bear the burden of proof that the request in question meets the conditions for refusal.

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

A business should take any reasonable steps needed to verify the identity of the person making the request to make sure that the person making it really is the consumer whose personal information is implicated. That being said, we believe that this verification should only be carried out to the extent that it is proportionate and necessary. In particular, a business should not require the requestor to submit copies of government-issued identification documents or credit cards if this is not proportionate to the risks associated with identity verification, particularly if it does not already have this information. It would be very helpful if the CPPA's rulemaking could specify that a business is not obligated to process additional personal information (information the business otherwise would not have) solely for the purpose of verifying the identity of the requestor.

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.*

Here we believe that the business should only reject a consumer's request to correct their own personal information in situations where this is demonstrably justified and, in such scenario, the business should be obligated to document this justification and include it in its records (unless there are overriding reasons why the justification should not be included). The burden of proof should always be on the business.

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.*

Aside from the protections already covered by the CPRA, where consumers opt out of their personal information being sold or shared or limit the use and disclosure of their sensitive personal information, and the business rejects their request, the business should be required to provide a strong justification as to why it continues to process the consumers' personal information in this manner despite the consumers'

objection. Here, the CPPA could provide guidance, *e.g.,* by including in its rulemaking a list of possible justifications, which could be expanded or otherwise amended as needed in future rulemaking.

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.*

We believe that this should cover personal information from which it may be possible to deduce or approximate sensitive personal information, but which would not *prima facie* constitute sensitive personal information unless further categorized or processed in some manner which identifies those sensitive characteristics. These categories could cover, for example, photographs or raw data which could imply protected categories of information, but where no actual categorization takes place. Similarly, behavioral or preference data which could indicate, for example, political views, would not necessarily be sensitive data, but should be treated as such once a categorization along those lines, either manually or through an algorithmic or AI process, is applied.

Furthermore, as we discussed on the subject of risk assessments above, sensitivity of personal information can be relative, and it can change depending on what other information it is linked or aggregated with. Any definition of 'sensitive personal information' should therefore also account for a situation when a particular piece of personal information is not 'sensitive' *per se* but becomes sensitive by virtue of its association with or links to other personal information (*e.g.,* pharmacy purchases, credit card transactions, visits to certain websites, physical location and movement patterns, *etc.*).

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.*

We would recommend keeping these situations narrow, in particular, due to the nature of information in question and the potential prejudicial effects it could have. The only situation where this disclosure should be possible is the presence of an overriding public interest in select areas (*e.g.,* contact tracing during an outbreak of a disease in the interest of protecting public health). At the same time, any such use or disclosure should only be done with appropriate safeguards in place, such as minimization, storage limitation and the use of privacy-friendly technologies such as encryption, de-identification or anonymization.

(iv) Definitions and Categories

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

If possible, we would like to see the specification that the definition of "personal information" also includes one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that consumer.

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

Here we believe that the definition could be expanded by including political opinions.

(v) Additional Comments

Lastly, we would like to highlight the fact that adopting rulemaking under the CPRA presents an opportunity to recognize security research as an important activity and a type of processing contributing towards continuously improving the ways of keeping consumers safe in an increasingly online-dependent environment. We believe that good-faith security research should be recognized under the CPRA rulemaking for the benefits it brings to consumers. Such recognition could take several forms (of which none are mutually exclusive):

a. The stipulation that, if duly disclosed, the of use personal information collected for the additional purpose of conducting security research is always compatible with the disclosed purpose for which the personal information was initially collected; and

b. The clarification that where a business, or a service provider or contractor, acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business, or service provider, or contractor to maintain the consumer's personal information in order to help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes, the phrase "to help ensure security and integrity" also includes carrying out security research (where this research may be also be private), all the while that conforming or adhering to all other applicable ethics and privacy laws.

4. Conclusion

We greatly appreciate having this opportunity to provide comments to the preliminary rulemaking under the CPRA. We would be more than happy to discuss any of the above suggestions with you in more detail. You can contact us at privacy@avast.com at your convenience.

Kind regards,

Avast Software Inc.

From: [redacted]
Sent: 9/23/2021 8:53:33 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 comment

[EXTERNAL]: [redacted]

Dear Ms. Castanon:

I am submitting this email as a preliminary response to the Agency's request for comment on the initial rulemaking process, pursuant to the notice issued September 23, 2021 (https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf). I may submit additional comments prior to the comment deadline.

I do not wish to have my name or contact information published as part of my comment. For your ease of reference, I shall place the portion of my comments that is okay to publish between dashed lines preceded by the phrase "begin public comment" and followed by the phrase "end public comment." If this is unclear for any reason, please let me know and I will attempt to clarify.

Begin public comment

As a professional writer, I have followed the passage of the CCPA, the development of its associated regulations, and the passage of the CPRA with considerable alarm, particularly with regard to their impact on free speech, free expression, and freedom of the press. **I am extremely concerned that these laws represent a significant threat to First Amendment rights, which OAG's previous rulemaking has done nothing to address or mitigate.**

This threat has several distinct aspects. First, the CCPA and the OAG regulations have sought to take an extremely broad view of what constitutes personal information subject to the rights established by these laws — MUCH broader than in prior California laws like the "Shine the Light" law or in the recently adopted consumer privacy laws of other states like Nevada, and considerably broader than what the average consumer would reasonably regard as "personal information." Thus, a wide range of information that the average person would probably not regard as personal information, and which could not reasonably be considered personally identifying, becomes subject to access, deletion, and opt-out requirements in the same manner as a driver's license number or private email address.

Second, the CCPA and the regulations issued by OAG have failed to make any meaningful allowance for the CONTEXT in which personal information is collected, adopting only an extremely narrow definition of publicly available information not subject to the rights defined by law. A reasonable person would likely recognize a substantive distinction between, for example, the collection and/or use of an individual's unpublished private phone number and the collection and/or use of a phone number the same individual publishes on billboards or hands out on business cards to everyone they meet; the law and its regulations do not. A reasonable person would likely also recognize a distinction between sensitive personal details recorded in a private diary and personal details the same individual publicly discloses in a bestselling memoir or newspaper interview. Again, these laws and the existing regulations make no such distinction.

Prior law and years of legal precedent have established the concept of "reasonable expectation of privacy," which provides some guidance for navigating these distinctions; the CCPA and CPRA have discarded that concept at a stroke.

By the CCPA/CPRA standard, simply reading a daily newspaper, watching a television interview show, or reading the published biographies of public figures becomes, in a legal sense, indistinguishable from a company like Facebook using tracking technologies to monitor an individual consumer's private Internet activity. Under these laws, an individual who posts a video of themselves on YouTube, an individual who appears in the background of a photograph or video taken on a public street during an event of public interest, and an individual surreptitiously photographed in their private bathroom at home all have precisely the same claim to privacy, which is fundamentally absurd and upends common sense understanding of what should be considered public or private information. I am frankly staggered that few people (and certainly not OAG) have seemed to recognize what a profound danger this presents to the First Amendment, or to any degree of public participation or free expression.

Third, the CCPA and OAG regulations do not recognize any intersection between public and individual interests with regard to the collection, processing, or disclosure of personal information. A reasonable person in a democratic society would likely recognize the distinction between an investigative reporter or biographer researching the life of a public figure or candidate for elected office and a company like Google compiling profiles of web users' online behavior to facilitate the sale of targeted advertising, but again, the law and regulations do not make or really even allow for any such distinctions.

In these ways, the CCPA and its existing regulations have created a perilous legal context in which the privacy rights defined by law can be wielded in a variety of ways that are obviously detrimental to free expression, free speech, and freedom of the press. For instance, a candidate for public office can now potentially use a "right to know" request to demand that a reporter disclose information gathered for an investigative report, and a public figure could use opt-out requests to suppress the publication of a book containing unfavorable information about them.

The CPRA compounds these risks in new and alarming ways. In adopting a "right to correct," the CPRA has sought to emulate the EU GDPR "rectification" right in ways that may be fundamentally incompatible with First Amendment rights in the United States. While there may be certain narrow contexts in which a rectification right might be appropriately applied (for example, with regard to the inclusion of incorrect facts in credit applications), **the most likely way this "right to correct" will be applied is in attempts to suppress unfavorable information and negative comments** in ways that fly in the face of California's previously robust anti-SLAPP protections. The distinction between information that is inaccurate and information that is truthful but unfavorable is not always a clear-cut one, but where such conflicts exist, particularly where they impact the public's right to know, the appropriate venue for resolving them is the courts, not a summary privacy request.

Creating an additional right to limit the use and disclosure of "sensitive" personal information throws gasoline on these fires. There are scenarios in which the exercise of such right might be appropriate (for instance, as a consumer, I would prefer that my bank does not share private details about my financial history with its marketing partners), but there are also many scenarios where apply such a right is clearly not appropriate. Let me present an illustrative example: Should it be possible for an openly gay public figure who is an officer of a labor union to demand that a publisher or a bookstore limit its use or disclosure of that information (which may be readily available to anyone with access to the Internet or who reads the newspaper) on the grounds that it constitutes "sensitive personal information" as defined by the CPRA? A reasonable person would likely agree that that would be absurd, and yet that is precisely the kind of demand the new law is inviting.

The fundamental problem with the framing of the CCPA, the OAG regulations, and the CPRA is that they clearly envision only one scenario: a business collecting nonpublic personal information about consumers purely for the business's commercial purposes, in a context that has no public impact outside of that business's relationship with consumers and consumers' individual rights. **The question you MUST ask yourselves is, "How might the application of these rights, or the Agency's enforcement approach, be abused in ways that are detrimental to First Amendment rights and/or public participation, and what steps can the Agency take to avoid or mitigate the potential for abuse?"** OAG did NOT do that, and it has made the CCPA a sword of Damocles dangling over free speech.

I recognize that the Agency does not have the authority to rewrite the statutes, but you do have the opportunity to approach your rulemaking with these considerations in mind, which OAG abjectly failed to do.

I have several additional points on your specific requests for comment, summarized below.

Section 2, Automated Decisionmaking

This provision of the CPRA, borrowed from the EU GDPR, suffers the same problem as the GDPR decision: a naïve and limited understanding (or lack of understanding) of modern technology. Much modern technology, particularly on the web, employs a variety of automated processes, from encryption and decryption standards to file compression to synchronizing data between different devices. How many of these processes could be called "decisionmaking" is debatable, they are innumerable, and they are often essential for the proper function and appropriate security of electronic systems. They may also be well beyond most users' technological understanding, and may in some cases constitute proprietary information subject to license agreements forbidding decompiling or reverse-engineering.

The Agency should take into account the following considerations:
1. The regulations should not be written so that they would have the effect of permitting individual consumers to opt-out of security, spam prevention, or identity verification procedures a business reasonably uses to protect its systems and/or data.
2. The regulations should not be written so that they would require a business to disclose information that is proprietary, that would violate the terms of applicable end-user license agreements, or that would compromise the security of the business's systems or data.
3. The regulations should not require businesses to possess or exercise an unreasonable degree of technological expertise. The average business operator is not a software developer; expecting them to understand and be able to explain in simple terms the decisionmaking involved in, for example, a human verification system like reCAPTCHA is probably unreasonable, and would be unhelpful to both consumers and businesses.
4. The regulations should allow businesses to decline to honor opt-outs that would present an unreasonable risk or obstacle to the business providing its services to the consumer.

Sections 4, 5, and 6:

As discussed in greater detail above, the Agency MUST consider how to frame these rules and procedures to mitigate the threat they present to free speech and freedom of the press and the public's right to know.

In particular, **the regulations pertaining to each of these rights must provide allowances for businesses to reject requests that would impact the exercise of First Amendment rights, the right of public participation, or the public good**. Under the CCPA, the right to delete does contain a First Amendment exemption, but that exemption does not go far enough, doesn't extend to the other rights except in a very narrow context, and was clearly not a priority for OAG.

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

In addition to the concerns discussed in greater detail above, the Agency should be careful that its regulations do not have the effect of requiring businesses to disclose specific pieces of information in ways that would violate copyright law or other laws or legal obligations regarding the disclosure of proprietary information, trade secrets, or other confidential information.

This is something that OAG has again abjectly failed to address, particularly with regard to published information in publicly available sources. For example, if the law regards information in published books or news reports as personal information subject to disclosure requirements, how is the business expected to respond to a request to know specific pieces of information? Requiring a business to create a catalog of every individual piece of personal information about a person that may be contained in a 300-page memoir or biography would in no way represent a reasonable expectation, nor is expecting a business to violate copyright law by sending the consumer a photocopy of every page in which the consumer is mentioned. (This problem would be mitigated to a significant degree by adopting a more expansive and sensible definition of what constitutes publicly available information not subject to disclosure, deletion, or opt-out requests.)

Similarly, **there has been little guidance to date of how businesses should deal with disclosure requests that involve information that is confidential**, e.g., subject to a nondisclosure agreement or a gag order issued by a court. I recognize that the Agency may be reluctant, even to the extent the statutory language permits, to allow businesses to deflect right to know requests with confidentiality agreements, but disclosing information subject to an NDA may subject a business to significant and potentially ruinous legal liability, so there has to be some effort to balance the consumer's rights with a business's other legal obligations.

Additionally, there has been little guidance on how to respond to "specific pieces of information" disclosure requests, or for that matter deletion or opt-out requests, where the specific pieces of information of several consumers overlap or are combined in ways that are difficult to separate: for example, a photograph or video in which several different consumers are visible.

A closely related question still unanswered: **To what extent should the exercise of one consumer's CCPA/CPRA rights be expected to override the expressed wishes, reasonable expectations, previously exercised rights, or wellbeing of another consumer?** Consider this illustrative example: Let us say that a publisher is preparing to publish an unflattering but truthful biography of a public figure that incorporates, *inter alia*, facts gleaned from the author's interviews with confidential sources close to that public figure. Should the public figure submitting a verified right to know specific pieces of information request require the publisher to disclose information from or about those interviews (e.g., recordings or transcripts) that would expose the identities of the sources, even though such disclosure would not only violate the publisher's promises of confidentiality, but could also expose those sources to actual harm? This is obviously not a scenario the authors of the CCPA envisioned, but it is nonetheless a relevant one that the existing rules invite and while failing to address.

This is of course a complex issue that may not lend itself to any "bright line" rulemaking, but the Agency MUST provide some guidance for how businesses are expected to approach this question in good faith. OAG has not.

Section 8: Definitions and Categories

The Agency should take care in not writing rules that would serve to undermine or invalidate existing good-faith efforts to deidentify or anonymize information.

For example, the Google Analytics service, a popular web analytics tool used by businesses to study the usage of their websites and apps, offers an IP anonymization feature that automatically removes the final portion of each user's IP address prior to processing. The partially redacted IP address is generally still sufficient to infer approximate geolocation (e.g., that a visitor is from a particular city), but is partially anonymized such that it is generally not possible to precisely locate or identify an individual visitor based on their IP address. This option was added to satisfy European privacy laws (particularly in Germany) and is widely used by businesses subject to the GDPR. If the Agency seeks to adopt a different and more stringent definition of "precise geolocation" that effectively invalidates this strategy, it would instantly undermine thousands of businesses' good-faith efforts to limit the specificity of their information-gathering, without necessarily providing any meaningful benefit to consumer privacy.

Similarly, **the Agency should be cautious that its regulatory definitions of deidentification do not create conflicts with the standard already applied to scientific and academic research**. Doing so could have a substantial chilling effect on such research and work done based on such research, which often has substantial value to the public interest, such as in matters pertaining to public health.

Regarding point 8e (combining information from different sources), I reiterate once again my substantial fears regarding the First Amendment implications of these laws. The Agency MUST approach its definitions and standards in this area with appropriate concern for the potential impact on free speech, free expression, and freedom of the press. For example, **stringent restrictions on combining information from different sources would have a devastating chilling effect on biographers, historians, documentarians, and reporters.** I would hope that the Agency would wish to avoid that.

Additionally, regarding methods for submitting requests, the Agency should take care (which OAG did not) to ensure that any requirements for methods of submitting requests be relevant to how a business actually conducts its business -- for instance, in not demanding that a business honor opt-out requests submitted via technological means that the business has no way to recognize or respond to. OAG made this mistake with its approach to "Global Privacy Control" signals. At the time the applicable regulations were published, the technical standards that define how Global Privacy Control signals are supposed to work was still a draft (and may still remain so), and there remain few if any commercially available solutions for reading and responding to such signals, but the confusingly worded OAG regulations had the effect of requiring businesses — even ones with no reasonable means to read the signals, much less translate them into action — to treat such signals as valid opt-out requests. This was foolhardy as well as unreasonable, and a prime example of what the Agency should avoid in its rulemaking.

Section 9, Additional Comments

An additional area of particular alarm regarding the CPRA, which did not appear to be mentioned in the invitation for comment, is the determination to impose GDPR-like rules limiting the retention of information.

The GDPR was written in a legal environment with significantly fewer protections for freedom of speech than U.S. law provides and also one in which tort law is significantly more restrictive. This should, and must, change the equation of what should be regarded as "reasonable" retention of information.

For example, under U.S. law, a business can face civil action related to its business activities at any time and from almost any imaginable jurisdiction. For that reason, it is customary -- and indeed good practice -- for many businesses to indefinitely retain business correspondence and other records. Without such records, a business may have little or no evidence to offer in response to a lawsuit, and since decisions in civil lawsuits in the U.S. are generally based on the preponderance of the evidence, the business would likely lose such a lawsuit. While some businesses do establish specific retention intervals for certain data, **the deletion of business information often carries a nontrivial degree of legal risk**, even absent specific legal requirements to retain certain data (e.g., tax returns) or ongoing contractual requirements. **The Agency should tread EXTREMELY cautiously in framing any regulation that may effectively demand that a business not retain its business records.**

Additionally, for journalists, writers, artists, historians, researchers, scientists, and academics, the information accumulated through research into past projects and prior work represents a valuable professional asset. For any creative professional, the prospect of being forced by California law to discard or delete interview transcripts, research notes, correspondence, old drafts, and other such information represents not only an unreasonable (and dire) threat to freedom of expression, but also a wholly unreasonable restraint of trade. **Should newspapers be forced to discard their clippings morgues and historians discard every research interview they conducted for past work as "no longer reasonably necessary for the original business purpose"?** Surely not, and yet there is a very real danger that the application of the CPRA rules could demand precisely that, which your Agency MUST take pains to avoid and mitigate.

As a final note, I want to emphasize my concern that **the CCPA, CPRA, and associated rules carry the very real risk of turning California into a preferred venue for pernicious attempts to deter public participation, fair criticism, and free expression**, and it is frustrating that the Legislature, OAG, and the authors of Prop. 24 seem either oblivious to or unconcerned about that danger.

Indeed, OAG's existing regulations for the CCPA are clearly written on the premise that any bad faith pertaining to the exercise of this law will be entirely on the part of businesses. There is certainly some risk of that, but little consideration has been given to the potential for harassment, frivolous requests (in particular through bogus requests submitted by the "bots" who gravitate to any web form to submit spam and abuse), fraud, and abuse by requestors, whose potential liability is minimal compared to the risk to the businesses they target. This has already been a problem with the CCPA, and the additional categories of rights created by the CPRA will make it worse.

Good public policy requires a good-faith balancing of interests, which in this case involves not only the rights of consumers, but also the rights and reasonable interests of businesses as well as the public interest. The CCPA, CPRA, and existing regulations have overwhelmingly favored the first consideration, but the second has clearly not been a high priority in prior rulemaking and the latter has received scant consideration. That MUST change, and it falls on your Agency to do so.

End public comment

From: Lelko, Marina [redacted]
Sent: 11/8/2021 9:44:10 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 Response to Proposed Rulemaking Under the CPRA of 2020
Attachments: CPRA Comment Call_11082021.pdf

[EXTERNAL]: [redacted]

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

Good morning,

SAFE Credit Union appreciates the efforts made by the Agency to seek input from stakeholders who very much want to aid in the protection of consumer data within reasonable guiderails to succeed in compliance.

Please see our attached preliminary comments on proposed rulemaking under the CPRA of 2020. Thank you for the opportunity to comment and for considering our views.

Best,
Marina Lelko | Compliance Manager
Direct: [redacted]
safecu.org | Let us put YOU first.

SAFE CREDIT UNION

Sacramento Business Journal Award
BEST PLACE TO WORK!
2018 - 2019 - 2020 - 2021

SAFE
CREDIT UNION

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 Debra Castanon:

I am writing on behalf of SAFE Credit Union (SAFE), which serves 13 counties in Northern California. We have over 240,000 members and over $3.8 billion in assets. SAFE respectfully submits the following preliminary comments on the proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA).

As a stakeholder, SAFE is interested in providing input on rulemaking and the efforts made by the California Privacy Protection Agency (CPPA) to collect comments on new and undecided issues not already covered by the existing California Consumer Privacy Act (CCPA) regulations. We have gone through the topics you have formulated to guide our comments.

Regarding the requirement for businesses to perform annual cybersecurity audits and submit to the Agency regular risk assessments about their processing of personal information, we request an exemption for financial institutions. Financial institutions are already heavily regulated and dedicated to the privacy of consumers and should be exempt from requirements of performing additional cybersecurity audits and risk assessments to the Agency. Presently, there are 12 IT/cybersecurity related exams, audits, and risk assessments (collectively referred to as reviews) that SAFE conducts or is subject to annually to ensure we are properly protecting consumer data. Below is a listing of those reviews either required by the National Credit Union Administration (NCUA) or supported by the Federal Financial Institutions Examination Council (FFIEC):

1. Gramm-Leach-Bliley Act (GLBA) / IT Data Risk Assessment
2. FFIEC Cybersecurity Assessment Tool, includes organizational size and complexity Inherit Risk Assessment and Cybersecurity Control Maturity Requirements and Assessment
3. Online Banking Risk Assessment
4. Disaster Recovery Testing/Assessment
5. Cybersecurity Incident Response Testing/Assessment
6. External Penetration Testing/Assessment
7. Internal Penetration Testing/Assessment
8. Wireless Penetration Testing/Assessment
9. Social Engineering Testing/Assessment
10. Cybersecurity Threat Risk Assessment
11. Information Technology General Controls Audit
12. NCUA/Department of Financial Protection and Innovations Exams

If no exemptions are possible for financial institutions, then the following resources should be a roadmap for items to be included in the cyber security audit and risk assessment:

- Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool
- National Credit Union Administration (NCUA) Cybersecurity Resources
- National Institute of Standards and Technology
- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Federal Deposit Insurance Corporation (FDIC) Cyber Security Resources

While the CPRA provides for regulations governing consumers' "access and opt-out rights with respect to businesses' use of automated decisionmaking technology" and/or "profiling," we would like to help increase distance between these two terms. We do not believe automated decisionmaking and profiling are interchangeable terms. Many companies use automated decisioning to determine if a consumer qualifies for a product or service. Profiling is taking consumers characteristics and matching products. Under no circumstances should a consumer be privy to or have access to a business' automated decisionmaking technology or "logic." Each business determines their own risk-based criteria and logic for an automated decisionmaking tool and providing this type of proprietary information may expose a business' vulnerabilities.

SAFE suggests the authority and scope of any audit conducted by the Agency be limited to the CCPA; on businesses that are not already regulated by provisions to protect consumer financial privacy in the Gramm-Leach-Bliley Act (GLBA) and, if applicable, the California Financial Information Privacy Act. If no such exemption can be made, then audits should only be conducted on a business if there are issues or valid claims of violations from consumers protected by the CCPA/CPRA.

The CPRA amendment to the CCPA to add a new right for consumers to request correction of inaccurate personal information should have certain reasonable limits so businesses may comply. It is reasonable to limit a consumer's request to correct their personal information to not more than twice in a rolling 12-month period. This aligns with the frequency and time frame that a consumer can make a request for their personal information from a business. As far as the process to make the correction, the CPRA should follow steps similar to the requirements in the Fair Credit Reporting Act that guides the consumer through a protective process to correct and dispute personal and credit information.

At no time should a consumer have direct access to a business's system to correct or delete information and records. Doing so may interfere with regulatory timeframes for retention the business manages. Another concern is that consumer's right to provide a freeform written addendum to their record with the business, if the business rejects a request to correct their personal information, would enable a consumer to disclose information not previously requested or required for business needs. This further obligates the business to categorize, track, and manage additional personal non-business-related information divulged by the consumer. It would interfere with, and elongate specific retention requirements that the business already has in place for destruction or archival of records.

SAFE appreciates the efforts made by the Agency to seek input from stakeholders who very much want to aid in the protection of consumer data within reasonable guiderails to succeed in compliance.

Thank you for the opportunity to comment and for considering our views.

Sincerely,

[redacted]

Sun Park
SVP, Enterprise Risk Management & Internal Audit
SAFE Credit Union

From: Jennifer Hodges [redacted]
Sent: 11/8/2021 10:58:49 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21 comments: Mozilla
Attachments: Mozilla's Comments to CCPA Consultation - November 2021.pdf

[EXTERNAL]: [redacted]

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

Dear Ms. Castanon:

Attached are Mozilla's comments on the California Privacy Protection Agency's preliminary rulemaking regarding the California Privacy Rights Act of 2020. Please let me know if you have any questions or need any additional information.

Thank you!

Sincerely,

Jenn Taylor Hodges

--
Jenn Taylor Hodges (she/her)
Head of US Public Policy
moz://a
[redacted]

Mozilla Corporation
2 Harrison St
Suite 175
San Francisco, CA 94105

November 8th, 2021

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

Re: Comments on proposed rulemaking under the California Privacy Rights Act of 2020 (PRO 01-21)

Dear Ms. Castanon:

Thank you for the opportunity to comment on the California Privacy Protection Agency's ("Agency") preliminary rulemaking regarding the California Privacy Rights Act of 2020 ("CPRA").[1]

Mozilla is the maker of the open-source Firefox web browser, the Pocket "read-it-later" application and other products and services that collectively are used by hundreds of millions of individuals around the world. Mozilla is also a global community of contributors and developers who work together to keep the internet open and accessible for all. As a mission-driven technology company and a not-for-profit foundation, we are dedicated to putting people in control of their online experience, and creating an internet that is open and accessible to all. To fulfill this mission, we are constantly investing in the security of our products and the privacy of our users.

General Comments

For Mozilla, privacy is not optional. It is an integral aspect of our Manifesto, where Principal 4 states that Individuals' security and privacy on the internet are fundamental and

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

Mozilla Corporation
2 Harrison St
Suite 175
San Francisco, CA 94105

must not be treated as optional. We actualize this belief by putting privacy first in our own products with features like Enhanced Tracking Protection (ETP)[2], Total Cookie Protection (TCP)[3], DNS over HTTPS[4] and our end to end encrypted Firefox Sync service.[5] We also promote privacy in our public advocacy, having engaged with privacy and data protection related issues across the world. [6]

Mozilla has long been a supporter of data privacy laws that empower people, including the landmark California privacy laws, California Consumer Privacy Act (CCPA)[7] and CPRA[8]. We're engaging today in support of the progress made thus far — but there's much more to do. The internet is powered by consumer data. While that data has brought remarkable innovation and services, it has also put internet users, and trust online, at substantial risk. We believe that everyone should have control over their personal data, understand how it's obtained and used, and be able to access, modify, or delete it.

Our comments below focus specifically on Global Privacy Control (GPC), which we are experimenting with within Firefox and we think can play an integral aspect in making a right to opt-out meaningful and easy to use for consumers.

---

[2] Latest Firefox rolls out Enhanced Tracking Protection 2.0, https://blog.mozilla.org/en/products/firefox/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default/
[3] Firefox 86 Introduces Total Cookie Protection, https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/
[4] Firefox continues push to bring DNS over HTTPS by default for US users, https://blog.mozilla.org/en/products/firefox/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/
[5] Privacy by Design: How we build Firefox Sync, https://hacks.mozilla.org/2018/11/firefox-sync-privacy/
[6] https://blog.mozilla.org/netpolicy/category/privacy/
[7] Bringing California's privacy law to all Firefox users in 2020, https://blog.mozilla.org/netpolicy/2019/12/31/bringing-californias-privacy-law-to-all-firefox-users-in-2020/
[8] Four key takeaways to CPRA, California's latest privacy law, https://blog.mozilla.org/netpolicy/2020/11/20/here-are-four-key-takeaways-to-cpra-californias-latest-privacy-law/

Mozilla Corporation
2 Harrison St
Suite 175
San Francisco, CA 94105

Response to Agency topic #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

Mozilla strongly supports the approach taken in the regulation to use settings at the platform level, particularly in web browsers such as Firefox, to allow consumers to opt-out of the sale or sharing of their personal information. Firefox today blocks third-party tracking. However, our technical protections are less suited for cases of first parties that might collect consumers' data and sell or share that data without the consumers' knowledge. As more browsers move to restrict cookies, we expect more websites to shift to this first party data collection and opaque sharing of that data behind the scenes.

Moreover, consumers cannot reasonably be expected to opt-out of the sale or sharing of their information individually from every party they interact with on the Internet. That is why a universal opt-out mechanism, set by the user, sent by the browser to all websites, and then enforced by the regulators, is so critical. Mozilla in October began experimenting with just such a setting: the Global Privacy Control (GPC), a feature available for experimental use in Firefox Nightly. Once turned on, it sends a signal to the websites users visit telling them that the user does not want to be tracked and does not want their data to be sold.

Unfortunately, the enforceability of GPC under CCPA remains ambiguous, with competing interpretations of do-not-sell requirements and with many businesses uncertain about their exact obligations when they receive a signal such as the GPC. The practical impact is that—**businesses may simply ignore the GPC signal**—especially if they have elected to use any other two mechanisms to receive opt-out requests.

History shows that without a clear legal mandate, most businesses will not comply with consumer opt-out signals sent through browsers. This vacuum is the same reason that

Mozilla Corporation
2 Harrison St
Suite 175
San Francisco, CA 94105

Do Not Track ("DNT") failed to gain adoption. It was eventually removed by all major browsers because it created a false sense of consumer protection that could not be enforced.

Mozilla encourages the California AG to expressly require business to comply with GPC. The 2023 Colorado Privacy Law has taken this step, and the addition of California would pave the path for other global privacy regulators to similarly update their laws. Further, enforcement authorities should expect businesses to interpret the GPC as governing both the direct sale of consumer's information as well as the sharing of consumers' information for programmatic advertising targeting purposes. Regulators, consistent with the intent of CCPA and CPRA, must step in to give tools like the GPC enforcement teeth and to ensure consumers' choices are honored.

Conclusion

We're grateful for the opportunity to share Mozilla's views in this preliminary submission and look forward to ongoing engagement with the Agency. We will seek to expand on topics of interest as the Agency continues stakeholder outreach and when new regulations and/or changes to existing regulations are published. If you have any questions about our submission, or if we can provide any additional information that would be helpful, please do not hesitate to contact us.

Sincerely,

Jenn Taylor Hodges
Head of US Public Policy
Mozilla

From: Kate Goodloe [redacted]
Sent: 11/8/2021 8:39:33 AM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
CC: Meghan Pensyl [redacted]
Subject: PRO 01-21 - BSA | The Software Alliance - Comments on Preliminary Rulemaking
Attachments: 2021.11.8 - BSA Preliminary Comments on CPRA Rulemaking - Final.pdf

[EXTERNAL]: [redacted]

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

Good morning,

Attached are comments from BSA | The Software Alliance responding to the invitation for preliminary comments on proposed rulemaking under the CPRA.

We appreciate the opportunity to provide these comments and would welcome an opportunity to discuss them or to respond to any questions that CPPA may have about them.

Best,

Kate Goodloe

Kate Goodloe
Senior Director, Policy
BSA | The Software Alliance
P [redacted]
W bsa.org

BSA | The Software Alliance

Submission to California Privacy Protection Agency On Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)

BSA | The Software Alliance appreciates the opportunity to submit comments in response to the invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 ("CPRA"). We appreciate the California Privacy Protection Agency's ("CPPA's") work to address consumer privacy and its goal of issuing regulations that better protect consumer privacy.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members are enterprise software companies that create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software.

Businesses entrust some of their most sensitive data—including personal information—with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations. Indeed, many businesses depend on BSA members to help them better protect privacy, and our companies compete to provide privacy-protective products and services. BSA members recognize that companies must earn consumers' trust and act responsibly with their data and their business models do not depend on monetizing users' personal information.

Our comments focus on six topics raised by the CPPA's rulemaking:

1. ***Cybersecurity Audits.*** New regulations are to require annual cybersecurity audits for businesses whose processing presents a "significant risk" to security; we urge the CPPA to define "significant risk" in line with, or by reference to, leading cybersecurity laws, policies and standards and further encourage the CPPA to leverage existing standards and best practices by allowing companies to satisfy this requirement by providing certifications, assessment reports, or other methods of demonstrating the use of practices consentient with leading standards and frameworks.

2. ***Risk Assessments.*** New regulations are to require businesses whose processing of consumers' personal information presents a "significant risk" to consumers' privacy to submit risk assessments to the CPPA; we urge the CPPA to define "significant risk" to privacy in line with leading global and state data protection laws and to focus on

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

requesting assessments from companies periodically rather than requiring all companies provide assessments to the agency on a standard timeframe.

3. ***Ability of Service Providers to Combine Information Received From Different Sources.*** New regulations may further define the business purposes for which service providers may combine information; we urge the CPPA to (1) ensure any new regulations do not disturb the careful business-service provider relationship set out in statute, and (2) avoid limiting the ability of service providers to combine information in ways that benefit consumers. We provide a range of examples illustrating how and why service providers may need to combine such information—without monetizing consumers' personal information or using it for advertising.

4. ***Automated Decision-Making.*** New regulations are to address the use of automated decision making in certain circumstances; we support reading this authority in line with the narrow statutory text, to focus the use of automated decision-making technology in the context of the access and opt-out rights already included in CPRA.

5. ***Agency Audits.*** New regulations are also to address the CPPA's audit authority. We urge the agency to limit the use of on-site audits in circumstances that present privacy and security risks, such as on-site audits of service providers that serve dozens or hundreds of businesses. We therefore encourage the CPPA to recognize potential alternatives to on-site audits, and to take steps to address privacy and security concerns that may be raised by an on-site audit in a particular instance.

6. ***Harmonizing the Regulations.*** We strongly encourage the CPPA to prioritize a harmonized approach to the new regulations—both for operational issues like opt-out mechanisms and for substantive issues where California's regulations may appropriately align with or build onto other leading global and state privacy laws. Doing so creates more clarity for consumers and drives investment by businesses into strong privacy programs that work across jurisdictions.

I. Cybersecurity Audits

Under the CPRA, regulations are to require businesses whose processing of personal information presents "significant risk" to consumers' security to perform annual cybersecurity audits. The statute identifies several factors to be used in assessing whether processing involves significant risk and states that regulations are to define the scope of the audit and establish a process to ensure that audits are "thorough and independent."[2]

BSA recognizes that data security is integral to protecting personal information and privacy. We focus on two threshold issues for the CPPA in implementing such regulations: (1) defining what processing presents a "significant risk" to security, and (2) leveraging existing cybersecurity audit and conformance processes and artifacts, including certifications and audit reports, that can satisfy the audit requirement.

A. Defining Significant Risk to Security

We encourage the CPPA to define processing that presents a "significant risk" to consumers' security in line with, or by reference to, leading cybersecurity laws, policies, and standards. These sources may help the CPPA to flesh out the CPRA's requirement that the definition of

[2] Cal. Civil Code 1798.185(15)(A).

"significant risk" consider the "size and complexity of the business and the nature and scope of processing activities."[3] These may include:

- **National Institute of Standards and Technology, Glossary – Definition of High Impact.** NIST has published a glossary of terms that defines "high impact" as: "The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in major damage to organizational assets; 3) results in major financial loss; or 4) results in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.)"[4] This definition builds on guidance in NIST-FIPS 199, which is used in categorizing federal information and information systems.[5]

- **Securities and Exchange Commission, Guidance on Risk Factors for Identifying Cybersecurity Risks.** The SEC has published guidance intended to help companies identify which cybersecurity risks should be disclosed. It contains a non-exhaustive list that can help companies to identify the risks that are significant enough to make investments speculative or risky. The eight criteria identified by the SEC include the probability of the occurrence and potential magnitude of cybersecurity incidents, the adequacy of preventative actions taken by the company to reduce cybersecurity risks, and the potential costs and consequences of such risks, including industry-specific risks and third-party supplier and service provider risks.[6]

Recommendation: The CPPA should define processing that presents a "significant risk" to consumers' security in line with, or by reference to, leading cybersecurity laws, policies, and standards.

B. Leveraging Existing Standards and Best Practices

We also encourage the CPPA to leverage existing standards and best practices for cybersecurity risk management, as well as established methods for demonstrating the use of practices consistent with leading security standards and frameworks. We encourage the CPPA to leverage these resources in two ways:

- ***First, any cybersecurity audit requirements should build on existing standards and best practices for cybersecurity risk management, including the NIST Cybersecurity Framework and ISO 27001.*** NIST's Cybersecurity Framework and ISO 27001 are the leading tools for organizations and governments to use in managing cybersecurity-related risks.[7] Although the Cybersecurity Framework was initially developed with a focus on critical infrastructure, such as transportation and the electric power grid, it has been adopted far more broadly by cross-sector

---

[3] Cal. Civil Code 1798.185(15)(A).
[4] NIST Glossary, available at https://csrc.nist.gov/glossary/term/high_impact.
[5] NIST – FIPS Pub. 199, Standards for Security Categorization of Federal Information and Information Systems, available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.
[6] Securities and Exchange Commission, 17 CFR Parts 229 and 249 (Feb. 26, 2018), available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.
[7] *See* ISO 27001, ISO - ISO/IEC 27001 — Information security management,NIST Cybersecurity Framework, available at https://www.nist.gov/cyberframework/framework.

organizations of all sizes and has been embraced by governments and industry worldwide. Likewise, as the leading global standard for information security, ISO 27001 is leveraged widely by organizations of all sizes. The CPPA should leverage these longstanding and trusted resources in implementing the audit regulation.

- ***Second, CPPA should allow companies to satisfy California's cybersecurity audit requirement by producing artifacts, such as certifications and audit assessment reports, that demonstrate use of practices consistent with existing leading security standards and frameworks***. Given the limited pool of existing auditors with sufficient security expertise, as well as the process involved in conducting a thorough audit, establishing new audit regimes is time-consuming and costly, especially for small businesses and technology consumers that may ultimately absorb such costs. We therefore encourage the CPPA to leverage existing leading security standards and frameworks whenever possible, which will ensure companies are complaint with high standards of data security while reducing both the time delays and costs of demonstrating such compliance. For example, many organizations may already implement strong data protection safeguards using leading security standards and best practices, including the NIST Cybersecurity Framework, ISO 27001, and Service Organization Controls (SOC) 2 Type 2 certifications. The CPPA's regulations should leverage certifications and reports that demonstrate compliance with those existing standards and frameworks. For instance, organizations may engage independent third-party assessment programs to obtain an ISO 27001 certification, which demonstrates conformance with ISO 27001 practices, or may obtain a SOC 2 Type 2 certification after an audit of certain controls like those focused on security or confidentiality, or may obtain FedRAMP authorization, which demonstrates conformance with practices consistent with the NIST Cybersecurity Framework (since both the NIST Cybersecurity Framework and FedRAMP baseline map to NIST 800-53, the U.S. Federal baseline for information security). Compliance with these standards and frameworks should satisfy California's cybersecurity audit requirement.

  We recommend the CPPA's regulations set forth the characteristics of cybersecurity certifications that meet CPRA's requirements and identify specific cybersecurity certification and audit frameworks that meet the requirements imposed by California's regulations, including ISO 27001, SOC 2 Type 2, and FedRAMP. The regulations should then provide that businesses complaint with ISO 27001, SOC 2 Type 2, or FedRAMP have satisfied the California cybersecurity audit requirement. Companies could demonstrate their compliance with these standards by producing a certification, attestation, or other artifact demonstrating compliance, including certifications or attestations by third parties. This approach enables California to leverage these existing thorough and independent certification programs and allows the CPPA to focus its own resources on organizations that have not obtained such certifications. Referring to existing standards also helps reduce fragmentation of privacy operations and enhances national and global harmonization on strong cybersecurity practices.

  In addition, thought should be given to the ability of smaller businesses that have yet to receive a certification to use records of a recent audit to demonstrate compliance with an adequate level of security.

Recommendation: The CPPA should leverage existing audit and certification procedures, including by: (1) building any audit requirements around the NIST Cybersecurity Framework and ISO 27001, and (2) allowing companies to satisfy cybersecurity audit obligations by

demonstrating compliance with existing leading security standards and frameworks, such as ISO 27001, SOC 2 Type 2, and FedRAMP.

II. Risk Assessment Requirements

Under CPRA, new regulations are to require businesses whose processing of consumers' personal information presents a "significant risk" to consumers' privacy submit to the CPPA "on a regular basis" a risk assessment. The statute identifies information to be included in that assessment and specifies that it does not require businesses to divulge trade secrets.[8]

BSA supports requiring businesses to conduct risk assessments for activities that are likely to result in significant privacy risks to consumers. We focus on two practical issues for implementing this requirement: (1) defining what processing presents a "significant risk" and (2) determining when such assessments should be provided to the CPPA.

A. Defining Significant Risk to Privacy

We encourage CPPA to define processing that presents a "significant risk" to consumers' privacy in line with other global and state data protection laws. Although California need not adopt a definition identical to those in other laws, the CPPA can benefit both consumers and businesses by adopting a definition of "significant risk" that aligns with other leading privacy laws. Supporting a consistent approach in identifying the types of data for which risk assessments are appropriate increases shared expectations about how consumers' data will be protected.

We highlight two potential approaches the CPPA could take in identifying processing that presents a "significant risk":

- **First, the CPPA could adopt a definition of "significant risk" modeled on the EU GDPR, by identifying criteria that companies are to use in determining if processing presents a significant risk.**

  The GDPR requires companies to conduct data protection impact assessments when processing is "likely to result in a high risk to the rights and freedoms of natural persons" —an assessment that takes into account the "nature, scope, context, and purposes of the processing." GDPR Article 35.3 also identifies three non-exhaustive circumstances in which assessments are required:

  (1) a systemic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling, that produces legal or similarly significant effects on a person;
  (2) large scale processing of special categories of data or data on criminal offenses; or
  (3) large scale systemic monitoring of a publicly accessible area.

  For other activities, companies are to determine if processing is high risk based on guidance endorsed by the European Data Protection Board (EDPB).[9] That guidance identifies nine criteria and suggests an assessment is required if two criteria are met. The criteria are:

  (1) the use of evaluation or scoring;
  (2) automated decision-making with legal or similar significant effects;

[8] Cal. Civil Code 1798.185(15)(B).
[9] *See* Article 29 Working Party, Guidelines on Data Protection Impact Assessments, endorsed by EDPB on May 25, 2018, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

(3) systemic monitoring;
(4) sensitive data or data of a highly personal nature;
(5) data processing on a large scale;
(6) matching or combining datasets;
(7) data concerning vulnerable data subjects;
(8) innovative use or applying new technological or organizational solutions; or
(9) when the processing itself prevents data subjects from exercising a right or using a service or contract.

To build on these criteria, data protection authorities (DPAs) in EU member states have created whitelists and blacklists of more specific processing activities intended to complement the guidelines.[10]

Benefits of the GDPR approach: This approach prioritizes identifying "high risk" or "significant risk" activities based on the context and substance of the processing. By using flexible criteria rather than a static list, it helps ensure the definition may be applied to new types of technology as they develop.

- **Second, the CPPA could define "significant risk" in line with the Colorado and Virginia privacy laws, by identifying specific processing activities that present significant risks.**

The Colorado Privacy Act requires companies to conduct risk assessments of processing that presents a "heightened risk of harm to a consumer," which is defined to include three scenarios:

1. Targeted advertising or for types of profiling that presents certain "reasonably foreseeable" risks;
2. Sale of personal data; or
3. Processing sensitive data.

The Virginia Consumer Data Protection Act is somewhat broader. It requires companies to conduct data protection assessments in four specific scenarios and includes a broader catch-all provision. Under the Virginia law, assessments are required for each of the following activities:

1. Targeted advertising;
2. Sale of personal data;
3. Processing that presents certain reasonably foreseeable risks;
4. Processing sensitive data; and
5. Processing activities involving personal data that present a "heightened risk of harm" to consumers.

Benefits of the Colorado and Virginia approach: This approach has the benefit of identifying specific scenarios that clearly require risk assessments, which sets clear expectations for consumers and clear implementation guidance for companies.

---

[10] *See, e.g.*, IAPP, EU Member State DPIA Whitelists, Blacklists and Guidance (last revised December 2019), available at https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/ (collecting guidance from DPAs); EU Member State DPIA Whitelists, Blacklists and Guidance (iapp.org); *see also* Muge Eazlioglu, IAPP Privacy Advisor, What's Subject to a DPIA Under The EDPB?, available at https://iapp.org/news/a/whats-subject-to-a-dpia-under-the-gdpr-edpb-on-draft-lists-of-22-supervisory-authorities/ (analyzing the EDPB's opinions on the lists of "high risk" activities by 22 DPAs).

Recommendation: We strongly encourage CPPA to adopt a definition of "significant risk" that aligns with the approaches embodied in other leading privacy and data protection laws. This will help ensure that companies conducting risk assessments focus their resources on the substance of the assessment and will support a common understanding of the types of processing activities that may present heightened risks to consumers.

B. Providing Risk Assessments to the CPPA

Under the CPRA, new regulations are to require risk assessments be submitted to the CPPA "on a regular basis."

We encourage the CPPA to adopt regulations stating this "regular basis" should be interpreted as meaning the risk assessments be provided to the CPPA upon request. This approach would allow the agency flexibility in requesting assessments from specific organizations and from broader categories of organizations for which the agency seeks to better understand the potential risks of processing. Adopting an alternative approach of specifying that all organizations are to submit risk assessments to the CPPA at a set interval, such as every two years or every five years, would create a potentially enormous quantity of assessments flowing into the CPPA that may not reflect the agency's priorities in identifying and addressing consumer harms. Reviewing those materials may also require such significant resources it could divert staff away from other important efforts by the agency.

In addition, the regulations should provide that the CPPA will treat risk assessments provided to the agency as confidential and not subject to public disclosure and make clear that the disclosure of those assessments to the agency does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections.[11] This will not only help to avoid inadvertent disclosure of proprietary data and business practices that may be reflected in a risk assessment, but also help ensure strong incentives for companies to undertake rigorous risk assessments.

Recommendation: We encourage the CPPA to define "regular basis" as meaning risk assessments should be provided to the agency upon request.

III. Business Purposes for Which Service Providers May Combine Consumers' Personal Information

Under the CPRA, new regulations may "further defin[e] the business purposes for which service providers . . . may combine consumers' personal information obtained from different sources."[12] Those regulations are subject to limits already imposed by the statute's definition of business purpose, which (1) excludes cross-context behavioral advertising, and (2) prohibits combining information for marketing and advertising purposes about consumers who exercised opt-out rights.[13]

We urge the CPPA to recognize the importance of ensuring that service providers can combine personal information received from different sources, including in ways that benefit consumers. Specifically, in crafting any new regulations the CPPA should: (1) avoid upsetting the business-service provider relationship set out in the CPRA, and (2) avoid limiting the ability of service providers to combine information in ways that benefit consumers. As described below, service providers often need to combine personal

[11] This protection is provided by other state privacy laws. *See, e.g.*, Colorado Privacy Act § 6-1-1309(4),Virginia Consumer Data Protection Act § 59.1-576.C.
[12] *See* Cal. Civil Code 1798.185(10).
[13] *See* Cal. Civil Code 1798.140(e)(6).

information to secure and improve the services they provide—without monetizing consumers' personal information or using it for advertising.

A. The Distinct Role of Service Providers

Because BSA members are enterprise software companies that often act as service providers under California law, we appreciate the care the CCPA and CPRA take in recognizing the distinct role of service providers that process data on behalf of businesses. Service providers are critical in today's economy, as more companies across a range of industries are undergoing digital transformations and depend on service providers for the tools and services that fuel such transformations.

Although the CCPA and CPRA primarily focus on businesses, which "determine[] the purposes and means of the processing of consumers' personal information,"[14] they recognize that businesses may engage service providers to "process[] information on behalf of a business."[15] Service providers must also enter into written contracts with businesses they serve, limiting how the service provider can retain, use, and disclose personal information provided to them by a business.

Distinguishing between businesses and service providers is important from a privacy perspective, because adopting role-based responsibility improves privacy protection. For example, by distinguishing between businesses and service providers, a privacy law can appropriately place consent obligations on the companies that decide how and why a consumer's data will be used—and are most likely to interact with the consumer. Businesses therefore have such obligations under CPRA, and they must enter into contracts with service providers that require the personal information remain safeguarded when it is processed on their behalf. This relationship ensures that the rights given to consumers and the obligations placed on businesses function in practice, in a world where both types of entities will handle consumers' personal information.

Recommendation: Any new regulations should not be read to upset the business-service provider relationship created by the text of the CCPA and CPRA.

B. Service Providers Need to Combine Personal Information

We urge the CPPA to recognize that regulations should not limit the ability of service providers to combine information in ways that benefit consumers. Indeed, businesses may ask service providers to combine information with other data sets, or to serve multiple businesses, for a range of purposes that benefit consumers and support responsible innovation—without monetizing consumers' personal information or using it for advertising.

These include:

- *Combining personal information to help protect and secure services*. In many cases, service providers identify cybersecurity threats and bad actors by combining information received from different businesses. For example, an email service that serves thousands of businesses may identify a bad actor attacking email accounts belonging to one business customer. However, by analyzing personal information across its services (by searching and combining elements of the underlying personal information stored on behalf of other businesses) the service provider can identify other email accounts of other businesses that may be targeted by the same bad actor.

[14] *See* Cal. Civil Code 1798.140(d).
[15] *See* Cal. Civil Code 1798.140(ag).

That information allows the service provider to proactively take steps to safeguard the at-risk accounts, and to increase the privacy and security of the personal information, benefitting both the businesses that use the email service and the consumers those businesses serve.

- *Combining personal information to make services work better.* Consumers and businesses often benefit from service providers combining personal information to improve their services. For example, a service provider may use personal information provided by one business to improve a service offered to many businesses—to the benefit of both the business customers and the consumers they serve. For instance, a service provider may create software that helps businesses manage customer service complaints, including by routing consumers with complaints to the employee team responsible for handling each type of complaint. That software will work better—and be more useful to both consumers trying to resolve complaints quickly and to businesses trying to satisfy their customers—if it is designed to identify patterns in how businesses route different types of complaints. By training the software on data collected from all of the businesses that use the software (instead of just on the data of one business), the software can become more efficient and effective, helping both consumers and businesses. The need to improve services based on personal information collected across business customers is not unique—it underpins many of the services that consumers and businesses rely on today.

- *Facilitating research.* Service providers can help entities conducting scientific research by combining multiple sets of data, at the direction of those entities and in line with privacy safeguards they have established. The resulting data could then be used to serve each of the participating entities.

- *Combining personal information to develop AI systems and to mitigate potential biases.* AI systems are trained with large volumes of data. Their accuracy—and benefits—depend on access to large amounts of high-quality data, which service providers may process at the direction of businesses. For example, a health care business may hire a service provider in connection with developing a fitness app that analyzes a consumer's heart rate to monitor for irregularities and predict whether the person is at risk of stroke or heart disease. To make the technology as accurate as possible, the business may direct the service provider to combine heart rate data from several publicly available health databases with data collected from the company's users in order to train the AI model. Directing the service provider to combine personal information collected by that business—which might disproportionately focus on one age group or ethnicity—with personal information available from other sources helps to mitigate against the risks of bias, benefitting both the consumers who will eventually use the service and the business customer. Regulations should not prohibit service providers from using or combining personal information for such purposes, at the direction of a business.

- *Combining personal information to serve multiple businesses at once.* There are many common scenarios in which businesses may ask service providers to combine information to provide a service to multiple businesses at the same time. We highlight two examples. First, in the case of a joint venture two businesses may jointly ask a cloud storage provider to store certain personal information together. Second, in the case of benchmarking services, consumers and businesses may seek out services that provide them context or help them understand how their activities fit into bigger trends. Consumers, for instance, may want to sign up for a program that allows their health care provider to combine their information with other sets of data, to better

understand potential health risk factors. Similarly, businesses may use benchmarking services to understand industry trends in hiring and human resources management, and to identify areas in which they may need to invest additional resources. Even when these services may only provide consumers and businesses with de-identified or aggregate information, they rely on the ability to combine personal information from which they derive the data to be shared. Regulations should not limit such uses, which continue to be subject to other safeguards in the CPRA.

- *Supporting open data initiatives.* More broadly, there is increasing recognition among governments and companies of the benefits of sharing data—subject to appropriate privacy protections. For example, the United States recently enacted the OPEN Government Data Act, which makes non-sensitive government data more readily available so that it can be leveraged to improve the delivery of public services and enhance the development of AI.[16] In addition, there is broad support for voluntary information-sharing arrangements, including by seeking to develop common terms so that companies that want to share data can more readily do so.[17]

Most fundamentally, any new regulations should recognize that in today's economy, service providers rarely work for a single business. Rather, service providers must efficiently and effectively provide products to hundreds or thousands of businesses at scale. Regulations that do not account for such relationships can inadvertently harm consumers that rely on these products and services, and the businesses and service providers that offer them.

Recommendation: The CPPA should ensure any new regulations (1) avoid upsetting the business-service provider relationship set out in the CCPA and CPRA, and (2) avoid limiting the ability of service providers to combine personal information in ways that benefit consumers.

IV. Automated Decision-Making

Under the CPRA, new regulations are to govern "access and opt-out rights with respect to business' use of automated decision-making technology, including profiling." Regulations are also to require that business' response to access requests include "meaningful information about the logic involved" in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.[18]

We encourage the CPPA to read this authority in line with the statutory text—which is phrased narrowly, and focuses on the use of automated decision-making technology in the context of the access and opt-out rights already included in CPRA. The plain language of CPRA accordingly calls for regulations that identify how those access and opt-out rights operate in the context of businesses using automated decision-making technology, including profiling. This reading of the statutory language is confirmed by the next part of the CPRA's text, which focuses on how the access right works in this context, by requiring businesses to provide "meaningful information about the logic involved" in such automated decision-making processes and a description of the likely outcome of such processes.

---

[16] *See* Public Law No. 115-435, Title II (Jan. 14, 2019).
[17] *See, e.g.*, Linux Foundation Debuts Community Data License Agreement (October 23, 2017, referencing IBM support), https://www.linuxfoundation.org/press-release/linux-foundation-debuts-community-data-license-agreement/.
[18] *See* Cal. Civil Code 1798.185(16).

Conversely, adopting a broader reading of this language would seem to exceed the statutory text, which does not envision regulations that contain the type of automated decision-making rights found in GDPR or the rights to opt out of certain types of profiling found in the Virginia and Colorado privacy laws.[19] While we appreciate the role that a strong data privacy law can play in ensuring that automated decision-making technology is used in responsible ways, and we believe focusing on these issues is needed as the underlying technology continues to be developed, the upcoming regulations do not appear to be the forum best suited to addressing these issues, given their narrow scope.

Recommendation: The CPPA should focus automated decision-making regulations narrowly, to address how the rights of access and the right to opt out operates in the context of businesses using automated decision-making technology.

V. Agency Audits

Under the CPRA, new regulations are to "define the scope and process for the exercise of the agency's audit authority."[20] The regulations are also to establish criteria for the selection of persons to audit and to protect consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.

We urge the CPPA to recognize the significant privacy concerns that may be raised by on-site audits, particularly in the context of service providers that serve dozens or hundreds of businesses, such as cloud computing providers. While we recognize the need for companies to provide appropriate information to regulatory agencies, on-site audits can raise specific security and privacy concerns, particularly in circumstances where they may expose information relating to a range of companies whose activities are not intended to be a focus for the agency.

As one example, an on-site audit of a company acting as a service provider for dozens or hundreds of customers may expose the on-site auditing team to a range of information that is not the subject of their efforts, unless the regulator and the company work to implement privacy and security safeguards regarding how information is to be reviewed on site. In the context of cloud services, for instance, on-site audits often provide very little information beyond that available through other sources, because the data most relevant to a regulator may simply need to be collected from servers—and is more efficiently reviewed and analyzed off-site rather than on the provider's premises. We therefore urge the CPPA to consider incorporating alternatives to on-site audits when an on-site audit raises meaningful privacy and security risks. Such alternatives may include permitting companies to submit information directly to the agency, so that it can be reviewed by the agency off site.

Recommendation: We urge CPPA to limit the use of on-site audits, particularly in circumstances where an on-site audit creates privacy and security risks. In addition, the CPPA should: (1) recognize potential alternatives to on-site audits, and (2) take steps to address privacy and security concerns that may be raised by an on-site audit in a particular instance.

---

[19] *See, e.g.*, GDPR Article 22 (stating that data subjects have a right "not to be subject to a decision based solely on automated processing . . . which produces legal effects concerning him or her or similarly significantly affects him or her"); Virginia CPDA Sec. 59.1-573 (creating a right to opt out of profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer"); Colorado Privacy Act Sec. 6-1-1306(a)(I)(C) (granting same right to opt out of profiling as Virginia law).

[20] *See* Cal. Civil Code 1798.185(18).

VI. Harmonizing the Regulations

Under the CPRA, the CPPA is to adopt regulations that harmonize approaches governing opt-out mechanisms, notices to consumers, and other operational mechanisms in order to promote clarity and functionality for consumers.[21]

We encourage the CPPA to prioritize harmonization across the upcoming rulemaking—which can better protect consumers and better support strong privacy practices for organizations.

- *For consumers, harmonized approaches to privacy regulation support a broader understanding of how privacy rights work in practice*. For this reason, we encourage the CPPA to consider how its proposed regulations may align with laws in other states and leading global privacy laws—and to choose regulatory approaches that align with or build onto the manner in which those laws implement consumer rights in practice. Of course, the context and perspectives around privacy and data protection appropriately vary among different legal frameworks—but supporting common approaches to core aspects of consumer privacy can help to decrease consumers' confusion about how to exercise their rights.

- *For organizations, harmonized approaches to privacy regulation also help drive investment in strong privacy programs that can satisfy the requirements of more than one jurisdiction*. In contrast, adopting regulations that are not designed to align with or build onto the manner in which other leading global and state privacy laws are implemented will fragment compliance efforts—a diversion of resources that should reflect an intentional choice rather than an unintentional consequence of creating regulations that do not account for existing laws, frameworks, and implementation mechanisms.

The CPPA has a unique opportunity to prioritize an approach to consumer privacy that is harmonized with other legal frameworks and soundly committed to maintaining high standards of privacy protection.

Recommendation: We strongly encourage the CPPA to prioritize a harmonized approach to the new regulations—both for operational issues like opt-out mechanisms and for substantive issues where California's regulations may appropriately align with or build onto other leading global and state privacy laws. This approach both creates more clarity for consumers and drives investment by businesses into strong privacy programs that can satisfy requirements of multiple jurisdictions.

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the CPPA on these important issues.

For further information, please contact:
Kate Goodloe, Senior Director, Policy
[redacted] or [redacted]

---

[21] *See* Cal. Civil Code 1798.185(22).

From: Serrato, Jeewon [redacted]
Sent: 11/8/2021 11:30:37 PM
To: Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]
Subject: PRO 01-21
Attachments: CPRA Comments November 8 2021 - BakerHostetler.pdf

[EXTERNAL]: prvs=7947f254f9=[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 Chairperson Urban:

We provide the attached submission in response to the California Privacy Protection Agency's invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020.

Thank you for your consideration. Let us know with any questions.

Jeewon

Jeewon K. Serrato
She | Her | Hers
Partner
Digital Transformation and Data Economy

BakerHostetler
Transamerica Pyramid Center
600 Montgomery Street | Suite 3100
San Francisco, CA 94111-2806
[redacted]

[redacted]
bakerlaw.com

BakerHostetler

Baker&Hostetler LLP

Transamerica Pyramid Center
600 Montgomery Street, Suite 3100
San Francisco, CA 94111-2806

T 415.659.2600
F 415.659.2601
www.bakerlaw.com

Jeewon K. Serrato
direct dial: [redacted]

November 8, 2021

VIA E-MAIL

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

Re: PRO 01-21

BAKERHOSTETLER'S COMMENTS IN RESPONSE TO INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING UNDER THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020 (Proceeding No. 01-21)

We provide the following submission in response to the California Privacy Protection Agency's (Agency) invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA).

To implement the law, the CPRA established the Agency and vested it with the "full administrative power, authority and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018." The Agency's responsibilities include updating existing regulations and adopting new regulations. In its September 22, 2021 invitation, the Agency sought input from stakeholders in developing regulations. The public was invited to submit comments related to any area on which the Agency has authority to adopt rules, but the Agency stated that it is particularly interested in comments on new and undecided issues not already covered by the existing regulations for the California Consumer Privacy Act of 2018 (CCPA).

BakerHostetler, one of the nation's largest law firms, represents clients around the globe. With offices coast to coast, our more than 1,000 attorneys litigate cases and resolve disputes that potentially threaten clients' competitiveness, navigate the laws and regulations that shape the global economy, and help clients develop and close deals that fuel their strategic growth.

We have six core practice groups: Business, Digital Assets and Data Management, Intellectual Property, Labor and Employment, Litigation, and Tax. Within these groups are several large specialty practices, including antitrust, bankruptcy, healthcare, energy, middle market mergers

and acquisitions, complex commercial litigation, data privacy and security, patent prosecution, and international tax. Our attorneys have broad knowledge and experience in many industries, including energy, media, manufacturing, healthcare, consumer products, hospitality, financial services and insurance.

BakerHostetler formed the Digital Assets and Data Management Practice Group (DADM Group) to mirror how our clients do business. Leveraging data and technology is a priority for most entities. We have united key service offerings and technologists to address all the risks associated with an entity's digital assets. Our clients are collecting data and then utilizing advanced technology to transform their products and services. Doing this creates enterprise risk. Our practice group works with our clients through the data life cycle – privacy, security, governance, transactions, emerging technologies and marketing and advertising – within an organization. The DADM Group comprises seven teams: Digital Risk Advisory and Cybersecurity; Healthcare Privacy and Compliance; Privacy Governance and Technology Transactions; Emerging Technology; Privacy and Digital Risk Class Action and Litigation; Advertising, Marketing and Digital Media; and Digital Transformation and Data Economy.

We provide comments below on the access and opt-out rights with respect to businesses' use of automated decisionmaking technology. Regulations related to automated decisionmaking will be critical for consumers to understand and exercise their rights related to automated decisionmaking and to help businesses to comply with CPRA.

Automated Decisionmaking

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

The CPRA uses several terms that relate to automated decisionmaking and/or profiling. Regulations that clarify the meaning(s) of the terms "profile," "profiling," "automated decisionmaking," and "automated processing" will help businesses comply with the CPRA. Based on the context in which these terms appear within the CPRA and the approaches taken under similar laws in other jurisdictions, we provide comments on how a "profile" should be defined as "the product or result of profiling." The regulations should also make clear that the phrases "automated decisionmaking" and "automated processing" mean the same thing in the CPRA and are both subject to the regulations to be promulgated under § 1798.185(a)(16).

- **The CPRA regulation should define the term "profile" to be "the product or result of profiling."**

The term "profiling" or "profile" appear four times within the CPRA. First, § 1798.140(z) of the CPRA defines "profiling" as:

> "any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section

> 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."

Second, the CPRA's definition of "personal information,", § 1798.140(v)(1)(K), includes as a category of personal information: "Inferences drawn from any of the information identified in this subdivision ***to create a profile*** about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." (Emphasis added.) Third, § 1798.185(a)(16) calls for the CPPA to promulgate regulations on automated decision-making and fourth, § 1798.140(e)(4) provides the following as a "business purpose": "[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 the consumer or otherwise alter the consumer's experience outside the current interaction with the business."

When it drafts the regulations under § 1798.185(a)(16), the Agency should clarify that each use of the term "profile" or "profiling" in the CPRA is understood to involve the application of automated decisionmaking and that a "profile" is the product or result of profiling. First, the fact that the term "automated" is included in the definition of "profiling" in § 1798.140(z) implies that there is only one type of profiling under the CPRA, and that the only way to create a "profile" about a consumer is through the means described in 1798.140(z). To treat the word "profile" as including non-automated means of processing personal information would result in inconsistency within the terms used by the CPRA and confusion among both consumers and businesses about when the creation of a profile resulted from the application of automated decisionmaking.

Second, the grammatical relationship between the noun "profile," the gerund "profiling," and both words' relationship to the verb "to profile" further supports the conclusion that when a business profiles a consumer, the result is a profile.

Third, any data that is generated through non-automated means would be better categorized as another category of personal information, rather than as a "profile." This will ensure that the category of "inferences" is reserved for the personal information that is drawn from automated processing of personal information.

For all these reasons, the CPRA regulations should clarify that a "profile" means "the product or result of profiling."

- **The CPPA should clarify that the terms "automated decisionmaking" and "automated processing" are synonymous.**

Section 1798.185(a)(16) of the CPRA provides rulemaking authority for "regulations governing access and opt-out rights with respect to businesses' use of ***automated decisionmaking*** technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer." (Emphasis added.) The term "automated decisionmaking" is not defined by the CPRA and is not used outside of § 1798.185(a)(16). Instead, the CPRA uses the term "automated processing." *See, e.g.,* § 1798.140(z) (defining "profiling" as "any form of ***automated processing*** of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185 (emphasis added)). Particularly because of the specific reference to § 1798.185(a)(16) within § 1798.140(z), it appears that the use of two different terms for the application of automated activities to personal information was likely not intended by the drafters of the CPRA. To avoid confusion among consumers and business and to clarify when and how its new regulations will apply, the Agency should specify that, within the CPRA and its implementing regulations, "automated decisionmaking" and "automated processing" mean the same thing.

- **The regulations should clarify that some applications of automated decisionmaking do not result in "profiling."**

The definition of the term "profiling" in § 1798.140(z) of the CPRA implies that "profiling" is the result of some, but not all, automated decisionmaking activities. Under the statute, "'Profiling' means any form of automated processing of personal information . . . to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." 1798.140(z). Under this definition, if an automated processing technology is for a purpose other than "to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements," it would not qualify as "profiling."

Drawing this distinction between "profiling" and automated processing would be consistent with the way "profiling" has been interpreted under the EU General Data Protection Regulation (GDPR). Under the GDPR, profiling is "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance as work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." (GDPR Art. 4.4) So, profiling under the GDPR requires automated forms of processing carried out on personal data for the purpose of evaluating personal aspects of an individual, such as that person's ability to perform a task, the person's interests, or the

person's likely behavior. The Article 29 Data Protection Working Party (the predecessor to the European Data Protection Board) clarified in its Guidelines on Automated individual decisionmaking and Profiling ("Article 29 Guidelines") that "profiling" under GDPR consists of the following three elements:

(1) it has to be an automated form of processing;
(2) it has to be carried out on personal data; and
(3) the objective of the profiling must be to evaluate personal aspects about a natural person.

To the extent the CPRA definition of "profiling" is inspired by the GDPR, it would be helpful to have regulations that clarify that "profiling" under CPRA must include substantially the same three elements:

(1) it has to be an automated form of processing;
(2) it has to be carried out on personal information; and
(3) the objective of the profiling must be to evaluate personal aspects about a natural person.

When comparing "profiling" with "automated decision-making," the Article 29 Data Protection Working Party Guidelines further state:

> "Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However, profiling and automated decision-making are not necessarily separate activities. Something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used."

Similarly, regulations that clarify that automated decisionmaking under the CPRA can be made without profiling would be helpful. To illustrate this point, we provide the following examples, as provided by the United Kingdom Information Commissioner's Office (UK ICO).

The UK ICO has stated that "automated individual decision-making is a decision made by automated means without any human involvement." *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/. To illustrate what "automated" could mean, it may also be helpful to refer to India's draft Personal Data Protection Bill (2019), which defines "automated means" as "any equipment capable of operating automatically in response to instructions given for the purpose of processing data," Section 2(6), Personal Data Protection Bill (2019).

Examples of automated decisionmaking may include:

a. An exam board using an automated system to mark multiple choice exam answer sheets, where the system is pre-programmed with the number of correct answers required to achieve pass and distinction marks. The scores are automatically attributed to the candidates based on the number of correct answers and the results are available online.

b. A factory worker's pay linked to their productivity, which is monitored automatically. The decision about how much pay the worker receives for each shift they work is made automatically by referring to the data collected about their productivity.

As illustrated by the examples above, not all automated decisionmaking has to involve profiling. According to the UK ICO, profiling can be used to:

(1) find something out about individuals' preferences;
(2) predict their behavior; and/or
(3) make decisions about them.

Examples of automated decisionmaking that involves profiling might include the following scenarios:

a. Medical treatments that apply machine learning to predict patients' health or the likelihood of a treatment being successful for a particular patient based on certain group characteristics.

b. Using social media posts to analyze the personalities of car drivers by using an algorithm to analyze words and phrases which suggest 'safe' and 'unsafe' driving in order to assign a risk level to an individual and set their insurance premium accordingly.

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.

CPRA does not provide any access requirements specific to businesses' use of automated decisionmaking technology. The access rights under CPRA would apply to businesses' use of automated decisionmaking technology to the extent the businesses are creating a profile about a consumer.

Under § 1798.110(a), a consumer has the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

- The categories of personal information it has collected about that consumer.
- The categories of sources from which the personal information is collected.
- The business or commercial purpose for collecting, selling, or sharing personal information.
- The categories of third parties to whom the business discloses personal information.
- The specific pieces of personal information it has collected about that consumer.

The Agency could clarify that a consumer's ability to access information about a business's use of automated decisionmaking technology would be limited to the access rights under § 1798.110(a). For example, if a business is creating a profile about that consumer, a consumer should be able to request that the business disclose the specific inferences it has collected about that consumer when it created the profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. Neither the CCPA nor the CPRA requires businesses to disclose to the consumers *how* the profile was created. The CPRA does, however, require businesses to disclose the categories of sources from which the personal information is collected. Businesses should comply with the CPRA to the extent it requires businesses to disclose the categories of sources from which the personal information is collected.

If a business sells or shares inferences, the business should also disclose that inferences, as a category of personal information, were sold or shared, as required by § 1798.115.

The CPRA also does not require businesses to provide a separate mechanism by which businesses must provide access rights to consumers to access information about the businesses' uses of automated decisionmaking technology. Regulations should clarify that businesses do not need to create a separate or stand-alone method for consumers to access information related to businesses' uses of automated decisionmaking technology. Consumers should be able to use the existing methods businesses have provided for making access requests for all personal information to exercise their access rights related to businesses' use of automated decisionmaking technology.

We acknowledge that this line of reasoning may not work outside of the CPRA. Rights provided under the GDPR and as interpreted by European data protection authorities rely in part on a distinction between automated decisionmaking and *solely* automated decisionmaking, which functions without human intervention. Under the UK ICO guidelines, for example, if a UK data subject is unhappy with a decision made using a solely automated process, they can ask for a review. The UK ICO has stated that organizations should explain how individuals can do this when they provide the decision that was made using solely automated decisionmaking. This right to request a human review and to contest decisions made using a solely automated process does not exist under the CPRA. We provide below further discussion about the opt-out rights under the CPRA.

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.

As stated above, CPRA's right to know and right to access requirements are enumerated in §§1798.110 and 1798.115. In response to a consumer's access request, a business should provide the information back to the consumers pursuant to requirements under §§1798.130(a)(3)(B) and 1798.130(a)(4). Responses to access requests from businesses should include:

- categories of personal information collected about the consumer;
- categories of sources from which the personal information was collected;
- the business or commercial purpose for collecting, or selling, or sharing the consumer's personal information;
- specific pieces of personal information obtained from the consumer;
- categories of personal information of the consumer that the business sold or shared;
- categories of third parties to whom the business sold or shared the consumer's personal information;
- categories of personal information of the consumer that the business disclosed for a business purpose; and
- categories of persons to whom the consumer's personal information was disclosed for a business purpose.

The CPRA does not have any separate requirements for businesses to disclose "meaningful information about the logic" involved in the automated decisionmaking process. The Agency should clarify that businesses should comply with the right to know and right to access requests, as enumerated in the CPRA under §§1798.110, 1798.115 and 1798.130.

This reasoning is acceptable because the rights afforded under the CPRA are different from the rights afforded by other laws, such as the GDPR. For example, in Italian Data Protection Authority (Italian DPA) decisions in 2021 involving automated decisionmaking and profiling, the Italian DPA found that neither the company's privacy policy nor its FAQs provided adequate information on how the system worked. The Italian DPA further found that EU data subjects have the right to obtain human intervention, to express an opinion, and contest the automated decision. Because of the transparency obligation of the GDPR, the Italian Supreme Court determined in a different matter that consent is only valid if there is adequate transparency of what the individual is consenting to when the consent is given, which means the algorithmic logic must be adequately explained to individuals in order to obtain valid consent.

The transparency and consent requirements as well as the right to contest the automated decision, however, do not exist under the CPRA. As stated above, the CPRA does not provide separate rights specific to businesses' use of automated decisionmaking technology or profiling. The Agency should provide regulations clarifying that businesses should provide "meaningful information about the logic" involved in the automated decisionmaking process to the extent it is required under §§1798.110, 1798.115, and 1798.130.

To offer another example from Europe, the UK ICO guidelines state that organizations should explain processes in a way that people will understand by providing "meaningful information about the logic" and "the significance and envisaged consequences" of a process. Organizations should describe:

- the types of information collected or used in creating the profile or making the automated decision;
- why this information is relevant to the automated decisionmaking or profiling process; and
- what the likely impact is going to be/how it's likely to affect the individual.

Again, this is UK guidance based on the GDPR. The CPRA regulations should limit its guidance to the requirements under the CPRA and not provide regulations that create new disclosure requirements that currently do not exist under the CPRA.

If the Agency is concerned about the harmful effects of the use of automated decisionmaking or deceptive practices, it may be helpful to note that the CPRA is not the only law governing privacy practices of businesses and the Agency is not the only regulatory body that will be regulating how businesses use automated decisionmaking technology. The Federal Trade Commission (FTC)'s 2021 AI guidance (E. Jillson, "Aiming for truth, fairness, and equity in your company's use of AI," Federal Trade Commission Business Blog, April 19, 2021 [Online]. Available: https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai) has stated that organizations cannot exaggerate an AI model's efficacy or misinform consumers about whether AI results are fair or unbiased. According to the FTC, deceptive AI statements are actionable. In fact, the FTC already provides that organizations building AI models based on consumer data must, at least in some circumstances, allow consumers access to the information supporting the AI models (*see* FTC, "Big Data – A Tool for Inclusion or Exclusion? Understanding the Issues," FTC Report, Jan. 2016 [Online]. Available: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf). The FTC has also stated that automated decisions based on third-party data may require the organization using the third-party data to provide the consumer with an "adverse action" notice (for example, if under the Fair Credit Reporting Act 15 U.S.C. § 1681 (Rev. Sept. 2018), such decisions deny an applicant an apartment or charge them a higher rent) (A. Smith, "Using Artificial Intelligence and Algorithms," Federal Trade Commission Business Blog, April 8, 2020. [Online]. Available: https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms).

We recommend that the Agency promulgate narrowly focused regulations that clarify the scope of the right to know and right to access requirements that apply to businesses under the CPRA. Like the limitations of the GDPR's Recital 63, Right of Access, which allows that the right of access "should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software," the Agency should provide regulations that explain that businesses need not provide any information to consumers

in response to access requests about automated decisionmaking process that would restrict a business's ability under one or more of the exemptions as outlined in § 1798.145.

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

Similar to the access rights, as outlined above, the statutory text of the CPRA does not provide for a separate opt-out right with regard to automated decisionmaking. The Agency should provide regulations that explain that consumers looking to exercise their opt-out rights under the CPRA have the following mechanisms to do so:

(1) right to opt out of sale or sharing of personal information under § 1798.120; or
(2) right to limit use and disclosure of sensitive personal information under § 1798.121.

Consumers also have a right of no retaliation following opt out or exercise of other rights under § 1798.125.

To facilitate opt outs, the Agency should provide regulations that clarify that a separate or stand-alone opt-out mechanism is not necessary with regard to consumers' opt-out rights with regard to automated decisionmaking. Businesses should allow consumers to exercise their opt-out rights with regard to automated decisionmaking using existing opt-out processes that exist for all opt-out requests relating to personal information.

Furthermore, the Agency should provide regulations that clarify that a separate or stand-alone mechanism is not necessary with regard to consumers' right to limit use and disclosure of sensitive personal information as it relates to automated decisionmaking.

Under the GDPR, businesses are restricted from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals unless certain exceptions apply, such as explicit consent or that it is necessary for entering into a contract. Unlike the GDPR, the CPRA does not provide for a similar distinction between types of automated decisionmaking. The Agency should clarify in its regulations that the opt-out rights provided to consumers under the CPRA are not limited to automated decisions that have a legal or similarly significant effect on individuals or that are solely automated (*i.e.* without human intervention). Opt-out rights, and all CPRA rights provided to consumers for that matter, should be provided to California consumers as long as the automated decisionmaking involves collection of personal information and profiling is carried out on the personal information with the objective of evaluating personal aspects about a natural person.

* * *

Thank you for the opportunity to submit preliminary comments on proposed rulemaking under the CPRA. Please do not hesitate to contact us with any questions you may have regarding our submission.

Jeewon K. Serrato
Partner

James A. Sherer
Partner

Shruti Bhutani Arora
Associate

Yeshesvini Chandar
Associate

Seungjae Lee
Associate

Tucker Sarchio
Associate

Whitney Schneider-White
Associate

Nichole Sterling
Associate

Justin Yedor
Associate