
From: Anthony Stark [REDACTED]
Sent: Monday, March 27, 2023 5:04 PM
To: Regulations
Cc: Bubba Nunnery
Subject: PR 02-2023 - ZoomInfo Comments on Draft CRPA Regulations
Attachments: ZI CPPA Comments 3_23.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear California Privacy Protection Agency:

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

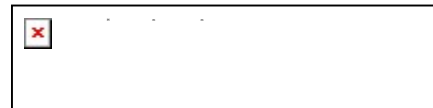
Warm regards,

Anthony Stark
General Counsel

O: [REDACTED]
E: [REDACTED]

805 Broadway St., Suite 900
Vancouver, WA 98660

www.zoominfo.com



March 27, 2023

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

Dear California Privacy Protection Agency,

ZoomInfo is a software and data company that provides information for business-to-business sales, recruiting, 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).

We are grateful for the opportunity to submit these comments as part of the rulemaking process for the California Privacy Rights Act (CPRA), and submit the following comments:

1. Cybersecurity Audits

We recommend the CPRA regulations provide that industry-standard cybersecurity certifications, such as ISO 27001, SOC2, or the NIST Cybersecurity Framework, be deemed an acceptable form of annual cybersecurity audit under the CPRA. One way to do it would be to describe it functionally and then to provide examples of current protocols that meet the definition. We believe these independent standards are designed by expert and well-meaning organizations seeking to set best practices in good faith and balancing considerations of all stakeholders. Therefore, leveraging this work should maximize both the efficiency and the effectiveness of an audit requirement. Businesses will be more likely to comply when they know what to do, and allowing them to follow an existing framework will give businesses that certainty. The regulations ideally would help businesses to identify best practices and provide a safe harbor for businesses who adopt those practices in good faith, incentivizing adoption and thereby maximizing the protective benefit provided to consumers.

2. Risk Assessments

We recommend aligning the CPRA's risk assessment requirements with those existing under other privacy regimes, including the GDPR and Colorado Privacy Act (CPA). Those laws provide that risk assessments should be conducted with respect to processing that is likely to result in "a high risk to the rights and freedoms of natural person." This aligns with the language set forth in the CPRA, which requires that a risk

March 27, 2023

assessment need only be conducted where the processing of personal data “presents a significant risk to consumers’ privacy or security.”

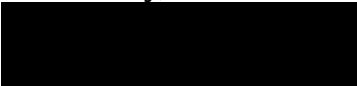

We further propose that “significant risk to consumers’ privacy or security” be interpreted in alignment with the GDPR, which provides that an assessment is required in instances of: (1) systematic and extensive evaluation of personal aspects relating to individuals that is based on automated processing, including profiling, and on which decisions are based that produce legal effects or similarly significantly affect the individual; (2) processing sensitive data on a large scale; or (3) systematic monitoring of a publicly accessible area on a large scale. We think this paradigm was carefully considered and appropriate, and aligning the CPRA to this paradigm will both protect consumers and provide consistency for businesses operating across jurisdictions who interact with individuals from multiple jurisdictions.

3. Automated Decisionmaking

We think the most important challenge in determining appropriate regulation of automated decision making is determining what “decisions” fall within the scope of what is regulated. We note that other regimes, including the GDPR and the Connecticut CTDPA provide that consumers may opt out of decisions that have **legal or similarly significant effects** on the consumer. We note that there are areas where we currently regulate decision making in order to prevent unlawful discrimination, for example, in lending, housing, and credit. We propose that this should serve as a starting point for the types of issues where additional scrutiny, assessment, and reporting is appropriate. While this is a highly complex issue, we do urge caution in defining the scope in a way that is overly broad or difficult for businesses to understand, as not all decision making has a significant impact on consumers. In all events, we urge alignment with the CTDPA, GDPR, and other state laws where it is reasonable to do so, in order to maximize compliance.

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

Sincerely,


Anthony Stark
General Counsel
ZoomInfo




From: Jill Szewczyk [REDACTED]
Sent: Monday, March 27, 2023 5:24 PM
To: Regulations
Subject: PR 02-2023
Attachments: 2023.03.27-Colorado Comments to CPPA.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good Evening.

Attached please find a comment from the Colorado Department of Law in response to the CPPA's Invitation for Preliminary Comments on Proposed Rulemaking.

Thank you,

Jill Szewczyk
Assistant Attorney General
Data Privacy and Security
Pronouns: She/Her/Ella



COLORADO
Department of Law
Attorney General Phil Weiser

P: [REDACTED] | [REDACTED]

The statements and opinions in this email do not represent the statements and opinions of the Attorney General.

PHIL WEISER
Attorney General
NATALIE HANLON LEH
Chief Deputy Attorney General
ERIC R. OLSON
Solicitor General
ERIC T. MEYER
Chief Operating Officer



STATE OF COLORADO
DEPARTMENT OF LAW

RALPH L. CARR
COLORADO JUDICIAL CENTER
1300 Broadway, 10th Floor
Denver, Colorado 80203
Phone (720) 508-6000
Consumer Protection Section

March 27, 2023

California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

RE: PR 02-2023, Invitation for Preliminary Comments on Proposed Rulemaking

The Colorado Department of Law (“CDOL”) thanks the California Privacy Protection Agency (“CPPA”) for the opportunity to provide comments in response to its Invitation for Preliminary Comments on Proposed Rulemaking: Cybersecurity Audits, Risk Assessments and Automated Decisionmaking. The CDOL supports the CPPA’s dedication to continued rulemaking in these areas.

We are proud that California and Colorado are leading the way in promulgating clear and effective privacy regulations, and appreciate the groundwork laid out by the California Consumer Privacy Act (“CCPA”) adopted rules, as well as the regulations established pursuant to the Consumer Privacy Rights Act (“CPR”). Additionally, we thank you for being active and engaged in the Colorado Privacy Act (“CPA”) rulemaking process. Your thoughtful comments throughout that process were invaluable as reflected by the final adopted CPA Rules.

Having promulgated rules on automated decisionmaking and data protection assessments as they apply to the CPA, we are grateful for the opportunity to share our rulemaking approach to these topics. We believe collaboration between the CPPA and the CDOL is beneficial and crucial to foster comprehensive privacy regulation that adequately protects consumers and facilitates compliance. We look forward to continuing our ongoing reciprocal support to ensure interoperability between our respective regulations.

Our comment seeks to (1) provide an update on the status of the CPA rulemaking, (2) describe Colorado’s data protection assessment requirements (“DPAs”), and (3) explain Colorado’s approach to defining and regulating automated decisionmaking.

Overview of the Colorado Privacy Act Regulations

On July 7, 2021, Governor Polis signed Senate Bill 21-190: Protect Personal Data Privacy, establishing the CPA, which is codified as part of Colorado’s Consumer Protection Act.

The CPA tasked the Colorado Attorney General with implementing and enforcing the CPA, granting the Colorado Attorney General the authority to promulgate such rules as may be necessary to administer the provisions of the CPA. The CPA also requires the Colorado Attorney General, by July 1, 2023, to adopt Rules that detail the technical specifications for one or more Universal Opt-Out Mechanisms that clearly communicate a Consumer’s affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for purposes of Targeted Advertising or the Sale of Personal Data pursuant to C.R.S. §§ 6-1-1306(1)(a)(I)(A) or (1)(a)(I)(B).

The proposed draft rules for the CPA were published by the Secretary of State on October 10, 2022, and the final rules were filed with the Secretary of State March 15, 2023. The CPA regulations were published in the Colorado Register on March 25, 2023, and will go into effect July 1, 2023.

Data Protection Assessment Requirements

The CPA risk assessment requirement is a key tool for identifying and mitigating processing risks related to consumer privacy. The CPA requires that entities conduct and document a data protection assessment (DPA) before conducting processing “that presents a heightened risk of harm to a consumer.”¹ The CPA Rules emphasize the need for meaningful DPAs that can help Controllers understand and proactively address the risks posed by their Processing activities. Part 8 of the CPA Rules highlights requirements regarding scope, stakeholder involvement, content, timing, and attorney general requests and CPA Rule 9.06 imposes DPA requirements specific to Profiling.

Considering both the need for meaningful assessments – as opposed to “check the box” exercises – and the wide variety of processing activities and business models among complying entities, the CPA Rules define the required scope of a DPA, but allow for flexibility as to the specific form.

Scope. CPA Rule 8.02 requires genuine, thoughtful DPAs that: 1) identify and describe the risks to the rights of consumers associated with the processing; 2) document measures considered and taken to address and offset those risks; 3) contemplate the benefits of the processing; and 4) demonstrate that the benefits of the processing outweigh the risks offset by safeguards in place.”

The CPA Rules attempt to encourage interoperability and avoid duplicative compliance efforts by allowing Controllers to use a DPA completed in compliance with another framework if it is “reasonably similar in scope and effect to the DPA that would otherwise be conducted pursuant to” the CPA Rules. A Controller may also supplement a previously prepared DPA with additional content required by Colorado.

¹ C.R.S. § 6-1-1309.

The CPA Rules consider challenges faced by smaller businesses by providing that the scope of a DPA should be “proportionate to the size of a controller, amount and sensitivity of personal data processed, and the processing activities subject to the assessment.” This recognizes that small businesses may have limited resources, but also indicates that a business’s size is only one factor that should be considered when determining the appropriate scope of a DPA.

DPA Triggers. Under the CPA, a DPA is required before a business or entity “conducts [p]rocessing that presents a heightened risk of harm to a consumer . . .” Unlike other frameworks, the CPA specifies that processing which presents a heightened risk of harm to a Consumer includes: (1) processing of personal data for targeted advertising or profiling that meets additional thresholds discussed below; (2) the sale of personal data; and (3) the processing of sensitive data.²

Content Requirements. The CPA Rules attempt to break down DPA content requirements into small, clear categories of information to provide an easier transition for companies coming into compliance. The rules reflect a balance between encouraging thoughtful exercise and flexibility for organizations to tailor DPAs to their own practices. CPA Rule 8.04 requires the following overarching categories of information: (1) a description of the processing activity; (2) the categories of personal data to be processed; (3) the context of the processing; (4) the nature and operational elements of the processing; (5) benefits; (6) risks; (7) safeguards; (8) a description of how the benefits outweigh the risks as offset by the safeguards; (9) internal and external parties contributing to the DPA; (10) information about audits conducted in relation to the DPA; (11) DPA approval information; and (11) information pertaining to a very specific CPA exception.

Harms. Within the DPA content requirements, the CPA Rules include a list of additional harms which should be considered, as applicable, when weighing the risks versus the benefits of a processing activity. The CPA Rules include that list to ensure that businesses and entities understand that processing can present some risks that may be less obvious than those addressed directly in the DPA thresholds, and to convey that the weighing of risks versus benefits includes an assessment of all “risks to the rights of the consumer[s] associated with the processing.”³

DPAs for Profiling. The CPA Rules include additional content requirements for DPAs required for profiling that presents a reasonably foreseeable risk of the specific harms outlined by the CPA. The Rules also attempt to clarify the relationship between the DPA requirements and those risks.

DPAs must be conducted in advance of profiling activities “if the profiling presents a reasonably foreseeable risk of: unfair or deceptive treatment of, or unlawful disparate

² C.R.S. § 6-1-1309.

³ C.R.S. § 6-1-1309(3).

impact on, [c]onsumers; financial or physical injury to [c]onsumers; a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of [c]onsumers if the intrusion would be offensive to a reasonable person; or other substantial injury to [c]onsumers.”⁴ CPA Rule 9.06 clarifies that threshold by describing the conduct covered by the terms “unfair or deceptive treatment”, “unlawful disparate impact”, and “other substantial injury.”⁵ The CPA Rules also provide that “Controllers should consider both the type and degree of potential harm to Consumers when determining if Profiling presents a reasonably foreseeable risk of “other substantial injury” to Consumers. For example, a small harm to a large number of Consumers may constitute “other substantial injury”.

To account for the unique risks of using automated processing and the opacity of automated processing systems, profiling-related DPAs conducted under the CPA must provide additional content pertaining to those specific risks. Additional required content listed in Rule 9.06(F) includes, but is not limited to: (1) “[t]he decision to be made using [p]rofiling”; (2) “[a]n explanation of the training data and logic used to create the [p]rofiling system, including any statistics used in the analysis, either created by the controller or provided by a third party which created the applicable [p]rofiling system or software”; (3) “[i]f the [p]rofiling is conducted by [t]hird [p]arty software purchased by the [c]ontroller, the name of the software and copies of any internal or external evaluations sufficient to show of the accuracy and reliability of the software where relevant to the risks described in C.R.S. § 6-1-1309(2)(a)(I)-(IV); (4) [a] plain language description of how the outputs from the [p]rofiling process are or will be used, including whether and how they are used to make a decision to provide or deny or substantially contribute to the provision or denial of financial or lending services, housing, insurance, education, enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services; and (5) “[h]ow the [p]rofiling system is evaluated for fairness and disparate impact, and the results of any such evaluation”.

DPA Submission. While the CPA Rules do not create requirements for DPA form or format, Rule 8.05 contains requirements for reviewing and updating DPAs, including that Controllers “shall review and update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of [p]ersonal [d]ata [p]rocessed and level of risk presented by the [p]rocessing, throughout the [p]rocessing activity’s lifecycle,” and that DPAs relating processing for profiling in furtherance of decisions that produce legal or similarly significant effects concerning

⁴ C.R.S. § 6-1-1309.

⁵ 4 CCR 904-3, Rule 9.06 explains that: (1) “[u]nfair or deceptive treatment” includes conduct or activity which violates state or federal laws that prohibit unfair and deceptive commercial practices”; (2) “[u]nlawful disparate impact” includes conduct or activity which violates state or federal laws that prohibit unlawful discrimination against Consumers; and (3) Controllers should consider both the type and degree of potential harm to Consumers when determining if Profiling presents a reasonably foreseeable risk of “other substantial injury” to Consumers.

a consumer “be reviewed and updated at least annually and include an updated evaluation for fairness and disparate impact and the results of any such evaluation.”

Stakeholder Involvement. Finally, the CDOL received pre-rulemaking and rulemaking input encouraging the CPA Rules to include DPA provisions relating to required stakeholder involvement. In response, Rule 8.03 requires that a DPA involve all relevant internal actors from across the controller’s organization structure, and where appropriate, relevant external parties, to identify, assess, and address the data protection risks.

Automated Decision Making – Definitions

The CPA and CPA Rules address automated decision making as it relates to profiling, which is defined in the CPA as “any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.”⁶ The CPA provides a right to opt out of “profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.”⁷

Definitions and Varying Responsibilities. Discrepancies regarding the scope of CPA profiling requirements were raised during the CPA rulemaking process. In particular, stakeholder comments included arguments both for and against limiting covered profiling to that involving solely automated processing, while others noted the interaction between human decision makers and automated tools like calculators and spreadsheets. In response, the CPA Rules offer a framework that attempts to balance opt-out rights and transparency related to profiling to help ensure that consumers understand and have control over the use of their personal data for decisions based on profiling. Specifically, the CPA Rules distinguish among different categories of automated processing, defining each category based on the level of human involvement and providing varying opt-out requirements based on the type of automated processing involved. Those categories of automated processing defined in Rule 2.02 are “Human Involved Automated Processing”, “Human Reviewed Automated Processing”, and “Solely Automated Processing”.

“Human Involved Automated Processing”, means the automated processing of personal data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the processing and (2) has the authority to change or influence the outcome of the processing.

“Human Reviewed Automated Processing” means the automated processing of personal data where a human reviews the automated processing, but the level of

⁶ C.R.S. § 6-1-1303(20).

⁷ C.R.S. § 6-1-1306(a)(I)(C).

human engagement does not rise to the level required for human involved automated processing. Reviewing the output of the automated processing with no meaningful consideration does not rise to the level of human involved automated processing.

“Solely Automated Processing” means the automated processing of personal data with no human review, oversight, involvement, or intervention.

The Right to Opt Out. CPA Rule 9.04 explains that controllers must honor a consumer’s request to exercise their right to opt out of profiling in furtherance of decisions that produce legal or other similarly significant effects concerning a consumer based on solely automated processing or human reviewed automated processing. Controllers do not have to act on a request to opt out of profiling based on human involved automated processing, but must provide information similar to that required in the controllers’ privacy notice (or a link to the section of the privacy notice containing that information).

Opt-Out Transparency. While the CPA’s right of access does not contain requirements specific to automated processing, the CPA Rules create disclosure requirements for controllers that process personal data for profiling for a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services. Specifically, CPA Rule 9.03 provides a list of disclosures that must be made in a controller’s privacy notice, and CPA Rule 9.05 provides a list of disclosures that must be made by a controller when requesting consent to process personal data for profiling if the profiling falls within the processing activities described in CPA Rule 7.02.

Conclusion

We hope that the CPA Rules provide helpful guidance as you continue to draft regulations relating to risk assessments and automated decisionmaking. We look forward to working together to safeguard the privacy and data security of consumers. Please do not hesitate to contact me if you would like to discuss further.

Respectfully submitted,

/s/ Jill Szewczyk

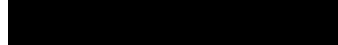
Jill Szewczyk

Assistant Attorney General

Colorado Department of Law

1300 Broadway

Denver, Colorado 80203



From: Barbara Lawler [REDACTED]
Sent: Monday, March 27, 2023 6:08 PM
To: Regulations
Cc: Barbara Lawler; Martin Abrams
Subject: PR 02-2023
Attachments: IAF Comments on CPPA Proposed Rulemaking - Risk Assessments and Automated Decisionmaking 03.27.2023.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,
Please find attached the IAF comments to PR 02-2023 CPPA Rulemaking for Risk Assessments and Automated Decisionmaking.

Regards,
Barbara Lawler

Barbara Lawler
President

[REDACTED]
www.informationaccountability.org





Information Accountability Foundation

RE: INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING For the California Privacy Protection Agency, PR 02-2023

The Information Accountability Foundation (IAF) is a non-profit research and educational organization headquartered in Los Gatos, California. It was created in 2013 to encourage fair information usage so that data pertaining to people might create real value for those people in a protective manner. The IAF is the incorporation of the [Global Accountability Dialog](#) that created "[The Essential Elements of Accountability](#)" that have been codified in the EU General Data Protection Regulation (GDPR), Colombia and Mexico privacy laws, and guidance in numerous countries. Accountability requires organizations to be responsible and answerable for their data use.

Assessments are central to organizations using data responsibly. Conducting assessments also create the record that organizations are accountable. To build accountability into advanced analytics, the IAF authored the "[The Unified Ethical Frame for Big Data Analytics](#)" that placed burdens on data users to assess the risk those organizations created for others. Since 2014, the IAF has worked with stakeholders to create assessment templates in the United States, Europe, Hong Kong, and Canada. The IAF work has inspired assessments in other jurisdictions as well. [Appendix Part B includes links to many of those assessment templates](#) and [Part C on Enforcement of assessments](#). The IAF currently is working on assessments that look to the full range of interests required by the final privacy rules just issued in Colorado. It is from that nine years' experience in developing assessments in collaboration with the full range of stakeholders that the IAF provides comments.

The IAF focuses its comments on Section II and III. The IAF uses the questions of the California Privacy Protection Agency (CPPA) as the starting point for the IAF's answers.

II. RISK ASSESSMENTS

1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumer' personal information require risk assessments?

Risk assessments related to the use of data pertaining to people come in many forms. There are privacy impact assessments (PIAs), data protection impact assessments (DPIAs), ethical assessments, legitimate interest assessments, and increasingly algorithmic assessments. PIAs were suggested strongly in 2012 by Canadian regulators [in "Getting Accountability Right Through a Comprehensive Privacy Management Program"](#). This document inspired similar documents in Hong Kong and Colombia. Many large Canadian organizations adopted PIAs in response to this regulatory encouragement. It was not a legal requirement. Those PIAs focused on data subject rights and today fall short of what seems to be required in the California law.

The GDPR requires legitimate interest assessments that balance the legitimate interests of the controller against the full range of rights and interests of the data subject. That requirement has had mixed

success both in governing legitimate interests as a successful legal basis and in bringing the full range of stakeholders into consideration.

The GDPR also requires DPIAs when a process creates “high risk” for data subjects. As referenced in the request for comments, the European Data Protection Board (EDPB) has published guidance on when and how to do DPIAs. While the EDPB guidance differentiates between risk to the organization, that is in part enterprise risk management, and risk to data subjects, the EDPB guidance doesn’t define what risk means. Given that gap, the IAF conducted a project called “Risk of What?” Are regulators looking for impediments to exercising data subject rights, such as transparency and data minimization, or inappropriate bad outcomes to people, as is the basis for the U.S. state and federal Fair Credit Reporting Acts (FCRAs)? Whatever the experience in Europe has been, it is inadequate because European regulators have not embraced totally Recital 4 of the GDPR which requires consideration of all stakeholders and the balancing of all fundamental rights.

In recent weeks, the Colorado Attorney General adopted final rules pursuant to the Colorado Privacy Act. Rule 8.04 provides guidance on Data Protection Assessment Content. Number 6 under that rule defines sources and nature of risks to the rights of consumers. That section seems to reflect the “Catalog of Problematic Data Actions and Problems” contained in the [“NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management.”](#) The IAF believes the NIST catalog is an excellent place to start when defining the risks to people and society when data pertaining to people is processed. The IAF used that catalog when developing its list of “Adverse Processing Impacts and Defining Risk” as part of the IAF model legislation, the [FAIR ANF OPEN USE ACT](#). The Agency may also find the [NIST CPPA-CPRA Crosswalk](#) helpful.

The chart below cross references the risks identified in the Colorado Rules against the IAF Adverse Processing Impacts.

Colorado Privacy Act Harms mapped to IAF Adverse Processing Impacts

Colorado Privacy Act Rules PART 8.04(6) – Privacy Harms	IAF-defined Adverse Processing Impacts <i>(Derived from NIST Catalog of Problematic Data Actions)</i>
a. Constitutional harms, such as speech harms or associational harms;	(9) Loss of autonomy and (10) Other detrimental or negative consequences
b. Intellectual privacy harms, such as the creation of negative inferences about an individual based on what an individual reads, learns, or debates;	(6) Stigmatization - Stigmatization or reputational injury
c. Data security harms, such as unauthorized access or adversarial use;	<i>Security breaches may cause outcomes from harmful processing that may take place when a breach occurs but are not a direct harm to individuals. Adequate security requirements should be covered elsewhere in a regulation.</i>
d. Discrimination harms, such as a violation of federal antidiscrimination laws or antidiscrimination laws of any state or political subdivision thereof, or unlawful disparate impact;	(8) Discrimination - Discrimination in violation of Federal antidiscrimination laws or in laws of any State
e. Unfair, unconscionable, or deceptive treatment;	Includes all adverse processing impacts including (4) Inconvenience or expenditure of time

f. A negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services;	(5) A negative outcomes or decision with respect to an individual's eligibility for a right, privilege or benefit – Denial of employment, credit, insurance, a license, etc.
g. Financial injury or economic harm;	(1) Financial Loss - Direct or indirect financial loss or economic harm
h. Physical injury, harassment, or threat to an individual or property;	(2) Physical Harm - Physical harm, harassment, or threat to an individual or property
i. Privacy harms, such as physical or other intrusion upon the solitude or seclusion or the private affairs or concerns of Consumers, stigmatization or reputational injury;	(6) Stigmatization - Stigmatization or reputational injury (9) Loss of Autonomy - Loss of autonomy through acts or practices that are not reasonably foreseeable
j. Psychological harm, including anxiety, embarrassment, fear, and other mental trauma; or	(3) Psychological Harm - Psychological harm, including anxiety, embarrassment fear, and other mental trauma
k. Other detrimental or negative consequences that affect an individual's private life, private affairs, private family matters or similar concerns, including actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used.	(10) Other detrimental or negative consequences

The IAF believes the CPPA should begin its regulations on risk assessments with a regulation similar to the rule enacted by the Colorado Attorney General. Having a set of common risks would enhance the ability for organizations of all sizes to get it right when trying to determine if a processing is highly risky.

The Colorado rule requires organizations to assess the risk to the individual to whom the data pertains, risk to groups of individuals, and risk to society as a whole. The business community has limited experience in looking beyond the risk to the business and the risk to data subjects. This comprehensive approach will require assessments begin with clearly thinking through and articulating the relevant stakeholders, how they might be impacted, and to what effect. The IAF believes that the Colorado rules will create the encouragement for that type of assessment to develop. As mentioned earlier, the IAF has developed templates for these types of assessments in the past.

Lastly, the EDPB guidance references the fact that organizations need to understand how to review their activities to determine whether a DPIA is necessary. The IAF believe that type of guidance would be useful as part of the regulations the CPPA issues.

2. What harms, if any, are particular individuals or communities likely to experience from a business's processing of personal information? What processing of personal information is likely to be harmful to these individuals or communities, and why?

The chart that is part of the answer to question 1 lists adverse processing impacts. What is missing from Question 2 is the harm to people of not processing information. Organizations make decisions every day to not process information pertaining to people because of compliance concerns related

to secondary use of data. Rules should be balanced to look at both sides of the risk equation. Are the data pertaining to people that do not get processed because they are a secondary use more or less harmful to society? Instead of a flat prohibition on secondary use, that kind of balancing should be done.

3. To determine what processing of personal information presents significant risk to consumers' privacy or security.

- a. What would be the benefits and drawbacks be of the Agency following the approach outlined in the EDPB's Guideline on Data Protection Impact Assessments.

As discussed above, the EDPB guidance only looks at the risk to the data subject, not the risk to other stakeholders. Also, the EDPB guidance does not catalog the risks that might come from the processing of data or not processing data. This balancing is important increasingly when determining the productive use of AI, the quality of complete data sets, and the concerns about profiling.

- b. What other models or factors should the Agency consider? Why? How?

The IAF suggests the CPPA consider Colorado Rule 8.04 that includes assessing the full range of stakeholders for the risk factors described in the rule.

- c. Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? Why, or why not? If so, how?

The IAF is not addressing cybersecurity issues.

- d. What processing, if any, does not present significant risk to consumer's privacy or security? Why?

Every time data pertaining to a person is used there is risk. Organizations should triage a processing to determine the level of risk both to the protection of the data and the protection of the people to whom the data pertains. It is the context for the use that ultimately defines the risk level. Whitelists and blacklists have limited utility in a fast-evolving world.

4. What minimum content should be required in business's risk assessments? In addition:

- a. What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under the GDPR and the Colorado Privacy Act?
- b. What, if any, additional content should be included in risk assessments for processing that involves automated decision making, including profiling? Why?

The IAF already has suggested that Colorado Rule 8.04 is a good place for the CPPA to start its rulemaking. The IAF is developing an assessment template for Colorado assessments that is not ready for this submission. The IAF also is developing the concept of assessing on the three dimensions of stakeholders, their fundamental interests, and adverse consequences to those fundamental interests.

Probabilistics, the basic process behind profiling, has been accelerating since the development of the first bankruptcy scores in the late 1980's. Automated decision-making is a natural development of quickly getting to decisions where probabilities are

clear. However, the fact that an outcome is probable is different than it being certain. The federal and state FCRA's have done a very good job of describing where decisions have a legal or similarly significant effect. Probabilistics add questions to the assessment process. There should be continuity from a base assessment to anything that needs to be added for profiling and automated decision-making.

5. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted businesses' submission of risk assessments that were complete in compliance with GDPR's or Colorado Privacy Act's requirements for these assessments? How would businesses demonstrate to the Agency that these assessments comply with CCPA's requirements?

Organizations already looking at where the GDPR and the Colorado requirements overlap and where they differ. It is impractical for organizations to conduct different assessments for the EU and Colorado (and California in the future). A Colorado assessment may begin with the GDPR factors and add the requirements related to the full range of stakeholders and adverse consequences in Colorado Rule 8.04. It would do the same thing with any additional California requirements. Fundamentally, the GDPR, the Colorado rules and the CPRA all call for the same thing: the conduct of assessments that consider whether risky processing is being conducted (risky processing includes the processing of sensitive personal data), evaluation of the benefits versus the risks of processing personal data for the business, its consumers, the public, and other stakeholder, and the avoidance of processing activities if they place significant potential risks on data privacy, outweighing its overall benefits.

The CPPA then should spot check assessments to make a judgement whether they were developed competently and with integrity.

6. In what format should businesses submit risk assessment to the Agency? In particular:
 - a. If business were required to submit a summary risk assessment to the Agency on a regular basis (as an alternative to submitting every risk assessment conducted by the business.

If organizations are required to submit every risk assessment to the CPPA, the CPPA will be flooded with submissions and will have limited ability to review those submissions. Informal conversations with organizations have led the IAF to believe that European agencies receive very few DPIAs because they must be submitted only if there is significant residual risk. Once risks are identified, organizations typically modify processing to mitigate those "significant risks."

The development of a summary risk assessment format should be a separate regulatory undertaking by the CPPA. Some jurisdictions are thinking about using the code of conduct process as a means for establishing the content of a summary assessment.

7. Should compliance requirements for risk assessments or cybersecurity audits be different for businesses that have less than \$25 million in annual gross revenues? If so, why, and how?

The IAF is not responding to this question.

8. What else should the Agency consider in drafting its regulations for risk assessments.

Organizations must develop a continuous process for determining the level of risk they create for others when processing data. There are discussions concurrently about fair AI assessments, ethical assessments, and algorithmic assessments. Risk assessments should be part of a

seamless process that begins with triage on whether a processing is going to create risks of adverse processing for identified stakeholders.

III. AUTOMATED DECISIONMAKING

The February 10, 2023, Invitation for Preliminary Comments asks a series of questions related to automated decision-making and profiling. The IAF is not responding to the specific questions but instead setting forth some basics for the discussion. The fact is that automated decision-making is baked into how things work on an everyday basis. For example, the CPPA uses automated decision-making on requests from browsers to access the CPPA's servers on a daily basis. These decisions have the effect of limiting who can browse the CPPA's website and file complaints. This is good because the alternative would be constant security breaches. However, the issues related to profiling and automated decision-making predate when consumer browsers made the Internet a consumer medium.

Martin Abrams, former Founder and President, currently the Chief Policy Innovation Officer of the IAF, was the President of the Centre for Information Policy Leadership (CIPL), the Vice President of Experian Policy Solutions, and the Assistant Vice President and Community Affairs Officer of the Cleveland Federal Reserve Bank. His background gives him the perspective to provide the following comments.

The consumer Internet accelerated an observational age that in turn accelerated the use of data for probabilistics pertaining to how people behave. The first broad-based probabilistic use of consumer data was probably the Fair Isaac credit risk score in 1989. It was quickly adopted by the consumer lending industry as an aid to better decisioning than was possible with the subjectivity of decisions made purely by lending officers. Soon that aid to people evolved into automated credit decisions. The U.S. Department of Justice (DOJ) investigated whether those decisions had the effect of making decisions on grounds that violated the Equal Credit Opportunity Act (ECOA). Since the data for credit risk scores came directly from credit bureaus, the FCRA required that the use of scores must be disclosed along with the factors that led to the denial. So, from the very beginning, the use of profiling and automated decision-making for substantive decisions were covered by a fair processing law, the FCRA.

In Europe, there was no uniformity in the data available for consumer credit decision-making. As Europe evolved towards the creation of the 1995 EU Privacy Directive, there were debates on whether it was unseemly for decisions on people to be made solely by a machine. Those concepts on what is seemly or not influenced the drafting of Article 22 of the GDPR. So, there are cultural differences between the way that Europe sees these issues and the way they are seen in the United States. The fact is that the relationship between profiling, the use of probabilistics against broad data sets, and automated decision-making is muddled still under Article 22 of the GDPR.

The 21st century saw the rise of analytic skills that allowed for the use of unstructured data into advanced analytic processes. Legacy statistics tested causality, while the growth of big data switched the dominant theme to correlation. This change naturally raised questions about the accuracy of the correlations, whether they were appropriate to apply, and whether they were influenced by the bias built into available data sets. This development has informed the debate about algorithmic fairness. These concerns have accelerated with the growing use of AI, which is the next stage of advanced analytics in our observational world.

So, in thinking about the questions the CPPA is asking, some pragmatic truths need to be addressed:

- Profiling is probabilistics built with consumer data. Building choice into the data that feeds the probabilistics has the unintended consequences of skewing the accuracy of predictive values. Choice worked when the relationship was one on one. Most relationships are no longer one on one. Ours is an observational world where there are not many one-on-one relationships. Choice no longer fits and indeed harms the process in an observational world.
- Automated decision-making is built into how many modern processes work, including the functioning of the CPPA's cybersecurity processes. Many automated decision-making processes are subject already to laws such as the FCRA, ECOA, and Fair Housing Act (FHA). The FCRA, ECOA, and FHA wrestled with these issues already and decided that the benefits of the automated decision-making outweighed the risks. Those Acts have methods for determining whether the automated decision-making is biased or not (after the fact testing), and those methods are just as applicable today as they were when they were implemented.
- Much of the emotions that pertain to automated decision-making are related directly to whether one thinks it is fairer for a person to make a decision or whether a well-governed algorithm, in the end, would be fairer. As mentioned above, the DOJ in the context of the ECOA decided that a well-governed algorithm was better.

The IAF staff believes this is where the discussion should begin. Thank you for the opportunity to contribute comments to this important rulemaking process.

Sincerely,

Martin Abrams, [IAF Chief Policy Innovation Officer](#)

Barbara Lawler, [IAF President](#)

Lynn Goldstein, [IAF Senior Strategist](#)

March 27, 2023

From: R. Jason Cronk [REDACTED]
Sent: Monday, March 27, 2023 7:54 PM
To: Regulations
Subject: PR 02-2023
Attachments: PR 02-2023 Enterprivacy Consulting Group.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please find the attached submission.

Jason Cronk

.....
[R. Jason Cronk](#) | JD, CIPT, CIPM, CIPP/US, FIP
Privacy Engineer | [Enterprivacy Consulting Group](#)
Chair and Founder | [Institute of Operational Privacy Design](#)
For Privacy Training <https://privacybydesign.training>
[REDACTED]

This letter is in response to the Agency's invitation to comment on its plans to issue regulations regarding the submission of risks assessment by businesses. I will address each prompt, in the request for comments, below. Not all prompts were responded to.

The CCPA directs the Agency to issue regulations requiring businesses “whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security” to regularly submit to the Agency a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits and risks of such processing. In determining the necessary scope and submission process for these risk assessments, the Agency is interested in learning more about existing state, federal, and international laws, other requirements, and best practices applicable to some or all CCPA-covered businesses or organizations that presently require some form of risk assessment related to the entity’s processing of consumers’ personal information, as well as businesses’ compliance processes with these laws, requirements, and best practices. In addition, the Agency is interested in the public’s recommendations regarding the content and submission-format of risk assessments to the Agency, and compliance considerations for risk assessments for businesses that make less than \$25 million in annual gross revenue. Accordingly, the Agency asks:

- 1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers’ personal information require risk assessments?**

While other commentors will no doubt include the GDPR, guidance from the UK ICO and others, I want to focus on the necessity of risk assessments in two other areas of best practice.

NIST Privacy Framework

The first is the NIST Privacy Framework, or more properly referred to as “NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE **RISK** MANAGEMENT.” The concept of understanding of privacy risk is central to the NIST Privacy Framework. Most other privacy standards and frameworks focus on principles or specific controls (GAPP, OECD, ISO 27701 to name a few). The NIST Privacy Framework proposed, as its Core, a set of 100 programmatic outcomes, many of which tie tangentially or directly to understanding privacy risk. Those outcomes are organized by five high level functions subdivided into 18 categories. One of those categories is

Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.

Two of the other categories (Data Processing Ecosystem Risks and Risk Management Strategies) are

principally devoted to managing risks and of the 18 categories, 13 of them mention risk management or dealing with privacy risk in their definitions. Suffice to say, understanding privacy risk and understanding risk assessments are crucial to the successful implementation of the NIST Privacy Framework. That being said, the use of the NIST Privacy Framework is voluntary and organizations whose choose to implement may cherry pick parts of the framework to use, but it would be difficult to extract the importance of the necessity of some degree of risk assessment without decimating the very tool a company may be trying to use.

Institute of Operational Privacy Design – Design Process Standard

The Institute of Operational Privacy Design (IOPD) published its Design Process Standard in January 2023. The standard takes a decidedly risk based approach. As a prerequisite, it requires that an organization identify a **Risk Model**. A Risk Model, in the IOPD standard, is defined as having identified threats, vulnerabilities and consequences and a methodology for measuring the likelihood of those factors and measuring the severity of the consequences.

The remainder of the standard contains 7 components, of which Manage Risk is by far the largest. The Manage Risk component is subdivided into two parts: performing risk assessments and responding to identified risks.

As with the NIST Privacy Framework, privacy risk is an integral part of the IOPD standard. And, again, similar to the NIST framework, the standard leaves open for interpretation the specific model and methodology to be used.

For the laws or other requirements identified:

- a. **To what degree are these risk-assessment requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(B)?**

Neither the NIST Privacy Framework nor the IOPD Design Process standard prescribe a specific risk assessment methodology. Both allow the organization to select a methodology that meets there needs (including regulatory obligations) to identify and react to privacy risk. An organization subject to CCPA could select an assessment method and risk model consistent with their obligations in California. For the NIST Privacy Framework, a crosswalk with CCPA has been developed, submitted to NIST and is hosted on the NIST website.

Category (Identifier):	Definition
Inventory and Mapping (ID.IM-P):	Data processing by systems, products, or services is understood and informs the management of privacy risk .
Business Environment (ID.BE-P):	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions .
Risk Assessment (ID.RA-P):	The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.
Data Processing Ecosystem Risk Management (ID.OE-P):	The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.
Governance Policies, Processes, and Procedures (GV.PO-P):	The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk .
Risk Management Strategy (GV.RM-P):	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Awareness and Training (GV.AT-P):	The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values .
Monitoring and Review (GV.MR-P):	The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk .
Data Processing Policies, Processes, and Procedures (CT.PO-P):	Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy .
Data Processing Management (CT.DM-P):	Data are managed consistent with the organization's risk strategy to protect individuals' privacy , increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).
Disassociated Processing (CT.DP-P):	Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).
Communication Policies, Processes, and Procedures (CM.PO-P):	Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks .

Figure 1 The 18 NIST Privacy Framework Core Categories with mention of risk highlighted.

b. **What processes have businesses or organizations implemented to comply with these laws, other requirements, or best practices that could also assist with compliance with CCPA's risk-assessments requirements (e.g., product reviews)?**

Unfortunately, most organizations have not adopted formal privacy risk assessment procedures. Those that have adopted something generally perform Privacy Impact Assessments (PIAs) or Data Protection Impact Assessments (DPIAs). The former, PIAs, tend to be post hoc justifications for the organization's activities, not a means of uncovering risk and addressing those risks. DPIAs, a term made popular by the GDPR's Article 35, tend to be limited, by the organizations implementing them, to circumstances proscribed by law. Article 35 specifies three high risk activities requiring a DPIA: when systematic large scale processing involved automated decision making resulting a legal effect, large scale processing of special categories of information and large scale systematic monitoring of public areas. EU based data protection authorities have adding their own specific circumstances which warrant DPIAs. Most organizations limit their DPIAs to those specific circumstances in the GDPR or identified by the data protection authorities, and make little effort to identify other areas of high risk processing that might warrant a DPIA. Further, when conducting DPIAs, the vast majority apply a superficial analysis which, unsurprisingly, supports the conclusion of continued processing with minimal mitigations.

Ero Balsa and Helen Nissenbaum, both of Cornell Tech, refer to this [performative compliance](#).

c. **What gaps or weaknesses exist in these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?**

By leaving the specific risk assessment up to the organization to decide upon, there is a near certainty that 1) the specific risks assessed are not robust enough to cover all of the consumer privacy risks created by the organization's activities and 2) the methodology chosen will be insufficient to properly measure the risks imposed on consumers.

Because privacy risk assessment research is still a rather nascent field, most organizations take a naive approach, focusing on organizational risk and not the external risks to consumers, often employing pseudoscientific home grown methodology with no objective basis. This tends to lead to the use of qualitative risk assessment with subjective interpretations ("health data? oh that's high risk." "over a million people? That's high risk."). These types of approaches suffer from a host of known deficiencies and would never be acceptable in industries with mature risk determination methods (insurance, finance, etc.). Common problems (from Michael Krisper's paper [Problems with Risk Matrices using Ordinal Scales](#)) include:

- **Incompleteness** – may not account for all essential factors influencing risk

- **Correlations** – selected factors could be correlated, over rating some risks and under rating others
- **Irrelevance** – irrelevant factors may cause work that doesn't influence the results
- **Non-linear Behavior** – factors may exhibit difficult to model non-linear behavior
- **Semi-Quantitative Scale Definition** – converting
- **Range Compression** – compression to a limited set of values can make various ranges appear to have parity with each other hiding variances in ranges such as uncertainty
- **Ambiguity** – borders between some ranges can be ambiguous (if medium frequency is weekly and high frequency is daily, where do you put something that happens every three days).
- **Neglecting Uncertainty** – compressing factors into classes mask uncertainty or variances in the population (if 90% of the population won't suffer any harm but 10% will suffer a critical harm, what's the overall harm to the population?)
- **Quantification Errors** – a slight increase in risk can result in risk measure going from say a 1 to a 2, appearing to double the risk, when in reality there was only a minor increase.
- **Human Bias** – Subjective determinations are highly biased by the rater who may be risk averse or have risk affinity bias. Humans also avoid extreme rating tending to gravitate towards middle of the road estimations
- **Human Inconsistency** – Humans are biased based on exterior factors and thus make inconsistent determinations, for instance rating a risk higher or lower depending on the immediate preceding rating they made, even though the determinations should be independent
- **Undefined Semi-Quantitative Arithmetic** – Risk assessments often attempt to apply arithmetic operations (additions, multiplication, etc.) to classes of risk factors with ordinal numbering schemes (ranked by order $1 < 2 < 3 < 4$). This can lead to illogical and meaningless results. We wouldn't accept this when applied to verbal descriptors (low risk plus high risk plus medium likelihood multiplied by highest impact means what exactly?).
- **Arbitrary Combinations** – should we add all risk or multiply them to derive overall risk? Should mitigations be subtracted from risk or divide? The decisions are often arbitrarily chosen
- **Neglection of Correlations** – Most risk assessment methods neglect correlations between events. Two seemingly low risk events, when they both happen to the same person could have catastrophic results. Two high risk events could in essence be the same results and thus not be any more risky than one independently.
- **Arbitrary Thresholds** – In grouping classes, people often choose arbitrary thresholds. If something affecting 1-99 people is low impact and 100-999 is medium impact why is the addition of the hundredth person that threshold? Why not 1-98 and 99-999? Why not 1-100 and 101-999?
- **Wrong Impression of Benefits** – Because many companies use similar pseudoscientific risk assessment methods, they appear authoritative. The use of numbers and mathematics gives the impression of rigor and "science." But these impressions lack basis in reality.

- **Deferred Feedback** – One of the biggest problems in risk assessments for privacy is they have no feedback loop. If an insurance company calculates flood risk for the following year, they can, over the next year look at actual flood data to estimate if their calculations were accurate. Over many properties and many years, those calculations can be refined and improved. Privacy risk assessment methods lack any such feedback loop.

While many regulators or other government bodies around the world (ICO, CNIL, NIST, etc) have attempted to provide guidance and even templates for companies to follow when conducting risk assessments, many of these also fall prey to the deficiencies listed above. For the most part the regulators (as with the companies) are not risk professionals. Their provision of these templates, unfortunately, provide an imprimatur of legitimacy on these methodologies.

- d. **What gaps or weaknesses exist in businesses' or organizations' compliance processes with these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?**
- e. **Would you recommend the Agency consider the risk assessment models created through these laws, requirements, or best practices when drafting its regulations? Why, or why not? If so, how?**

As previously mentioned, both the NIST Privacy Framework and the IOPD standard leave subject to interpretation the specific risk assessment method, so there is little in the way of guidance for the Agency. However, I do want to comment here on the recommendations and guidelines issues by regulators for compliance with other laws (such as GDPR). Unfortunately, these recommendations, because they suffer the flaws mentioned above should not be a model adopted by the Agency.

- 2. **What harms, if any, are particular individuals or communities likely to experience from a business's processing of personal information? What processing of personal information is likely to be harmful to these individuals or communities, and why?**

A complete exploration into the harms of processing of personal information is beyond what can be submitted here. I suggest a reading of Danielle Citron and Daniel Solove's Privacy Harms paper. The Future of Privacy Harms also has a good white paper on Distilling the Harms of Automated Decision Making which is widely applicable.

One key point I'd like to make is to avoid, and avoiding allowing companies, to focus solely on tangible harms (identity theft, financial harms, reputation, etc.). Privacy has a social/moral context that cannot be understated. GDPR repeatedly makes use of the phrase "rights and freedoms" and

measuring the likelihood and severity of those situations. Similarly the CCPA should encourage, and demand, risk assessments that consider the likelihood and severity of intangible violations of privacy. A visceral example will provide some context. If an internet connected in home security camera is compromised to record the nude photographs of an occupant and those photos are distributed around the globe, few among us would deny a violation of the privacy of the occupant has occurred. In this scenario, there is a likelihood attributable to such an event (the probability the camera will be compromised, the probability the occupant will be nude in front of the camera and the probability the hacker will record those and distribute them). One can also attribute a severity to that violation (possibly by surveying people on their views of how bad the invasion is say contrasted against other scenarios, such as a photographer capturing photos of people at a beach or in other situations). In other words, you can calculate risk associated with that camera in the home. Now, there are risks of subsequent tangible harms (the person finds out and is embarrassed, they lose a job or employment opportunity, etc) but even without those, the hackers intrusion is a privacy violation and there is a risk of that violation that can be measured and mitigated against. The problem of focusing on the tangible harms is that firms can mitigate those while still leaving the underlying violation. Facebook, for instance, in was revealed during discovery for one of their lawsuits, was concerned about people being disturbed by Facebook scanning of SMS messages which might result in them deleting the Facebook app from their phone. Rather than curb the underlying activity (looking at SMS messages) they suppressed alerts in the phone so people weren't aware and thus didn't have a tangible reaction.

Similarly, under CCPA a firm might calculate the risk associated with a person's inability to exercise a right if that firm shares data with a vendor (vendor is in a foreign country, defies their contractual obligations, etc.). If focused on tangible impacts, a risk assessment might reduce the results by saying only 1 in 100,000 Californians will try to exercise this right, thus the risk is "low" of someone tangibly being denied their rights. However, if the assessment reviews the intangible risk of the vendor cannot or would not follow through on their obligations, if presented with a rights request, the likelihood may be "high" for certain vendors and the severity high because a right afforded under California law would not be available. Note, the use of low and high aren't not meant to convey any approval of these terms as applied to a risk assessment but to forgo a quantitative analysis on a hypothetical situation.

3. To determine what processing of personal information presents significant risk to consumers' privacy or security under Civil Code § 1798.185(a)(15):

- a. **What would the benefits and drawbacks be of the Agency following the approach outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessment?**

The most striking problem in following the EDPB's guidelines is that most companies restrict themselves to an analysis of the enumerated situations in the guidelines or those identified by other member state supervisory authorities. The second problem is that organizations generally lack a sophisticated view of how risk to "rights and freedoms" flows from data processing activities. The EDPS survey of DPIA activities in EU institutions sheds some light:

This is supported by the following statement by a DPO: “In general the point of view of risks to the data subjects, not to the agency. When it comes to the DPIA, justification based on business activities instead of adopting the point of view of the data subjects should be the main driver. Unfortunately, it is not the case. Also, the risks towards the ‘rights and freedoms’ of the data subjects is a concept difficult to be grasped, as there is no immediate connection between the processing of personal data and how adversely that could affect rights and freedoms. [Emphasis added] Data processing is seen as something ethereal that has no direct impact on the lives of the data subjects, and if so happens, it is only limited cases under exceptional circumstances”.

Another telling fact, is that when most companies conduct a “risk assessment” of even activities that the EPDB and supervisory authorities define as “high risk” they almost invariably conclude that there is little risk or that the residual risk has been sufficiently reduced and continue with the activities unabated. This is not an indictment that the regulators’ base assessment is wrong, but rather a illustration that the assessment process is purely performative and lack critical or substantive review.

A lot of professional throw around the terms “privacy risk” and “high risk” or “low risk,” without a clear articulated understanding of what that means. This includes many of the European regulators. This lack of supporting definitional structure leads to ambiguous phrasing in their guidance which leads to further ambiguity in the regulated entities. For instance, Article 35 suggests that large scale processing of special categories of personal data (i.e. “sensitive” data) is, de facto, high risk. Why? Dan Solove, renowned professor of privacy law at George Washington University, in his recent paper [“Data Is What Data Does: Regulating Use, Harm and Risk Instead of Sensitive Data”](#) makes the excellent case that categorization of data as “sensitive” (“special categories” in GDPR parlance) masks real harms, ignores inferences, oversimplifies analysis and can lead to absurd, counterintuitive, results.

The GDPR, itself, illustrates some of the problems of this short-sighted analysis. Recital 51 includes the phrase “[t]he processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.” However, such disregards that photographs of people often can lead to inferences about those people, such as gender identity, sexual orientation, ethnicity, and other qualities. The regular and systematic inclusion of photographs in resume in a job site could led to discrimination. The aggregation of data (say from submitted resumes without photos) combined with photographs from social media of candidates could be unexpected behavior on the part of a job board. The drafters of the GDPR realized that photographs as special categories of data would be highly problematic given the ubiquity of photos on the Internet and thus tried to walk a fine line. However, this then hides the fact that there are risks and those risks are, in some cases, significant.

Another example, from recent events, is whether social media companies anticipated that a facial recognition company would scrap photos of individuals to develop algorithms to support law enforcement and private companies' need for facial recognition. I'm speaking about [Clearview AI](#). A proper risk assessment would have elucidated and measured this potential and pointed the way to mitigating/compensating controls. But the constrained methodology promoted by the various data protection authorities in the EU are too narrow in scope and too crude to do so.

b. **What other models or factors should the Agency consider? Why? How?**

The academic literature on privacy risk is still in its infancy. Several different methods are currently being circulated and discussed:

- * MITRE's Stuart Shapiro's STPA-Priv (System-Theoretic Process Analysis for Privacy)
- * LINNDUN Threat Modeling and [Privacy Risk Assessment for Data Subject Aware Threat Modeling](#)
- * From myself and Stuart Shapiro, an application of [FAIR \(Factors Analysis of Information Risk \) to privacy](#)
- * MITRE is working on a [privacy threat model](#), similar to their cybersecurity [ATT&CK model](#).

This [article](#) is informative. The Agency should support efforts to develop sophisticated **science-based** risk models and assessment methodologies.

c. **Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? Why, or why not? If so, how?**

There are several key distinctions between cybersecurity risks and privacy risks. First and foremost cybersecurity risk have an immediate effect and the target of the risk is the organization (hacker's compromise the organization's systems, a power failure shuts down the organizations IT systems, a hard drive corrupts the integrity of the organization's data), where as in privacy risk the at-risk entity is the person, with organizations being secondarily affected through regulatory action, brand damage or legal action. Secondly, privacy is much more contextual than security. If I covertly install a camera in your home, that's a privacy violation. If you invite me to do so to monitor your home while you're vacation, I now have a viable business service that you'll pay me for. Thirdly, often the organization or parts of it may be the initiator of privacy risk (referred to at the threat actor). There may be business incentives driving privacy invasive activities (such as monetization of data). Whereas in cybersecurity risks that also affect consumers the incentives with the business are often aligned, in privacy risks their may be opposing incentives for a business not to act on privacy risks. In both cases of the camera example mentioned above, security of the camera is important. In the former, I don't want you finding the camera or breaking the network to stop my covert surveillance. In the latter, we both don't want hackers to infiltrate the

camera and learn when you're not home to possible rob your house. Because of the misalignment of interest, privacy risk assessment need, ideally, independent review with a critical eye. This was supposed to be the role of the quasi-independent DPO under GDPR, but often times a DPO who provides critical analysis will not last long in a role. This was probably one of the reasons behind the EPDB's launch of a coordinated effort to review the appointment of DPOs in September of 2022.

- d. What processing, if any, does not present significant risk to consumers' privacy or security? Why?**

4. What minimum content should be required in businesses' risk assessments?

In addition:

- a. What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act?**
- b. What, if any, additional content should be included in risk assessments for processing that involves automated decision making, including profiling? Why?**

5. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted businesses' submission of risk assessments that were completed in compliance with GDPR's or the Colorado Privacy Act's requirements for these assessments? How would businesses demonstrate to the Agency that these assessments comply with CCPA's requirements?

6. In what format should businesses submit risk assessments to the Agency? In particular:

- a. If businesses were required to submit a summary risk assessment to the Agency on a regular basis (as an alternative to submitting every risk assessment conducted by the business):**
 - i. What should these summaries include?**
 - ii. In what format should they be submitted?**
 - iii. How often should they be submitted?**
- b. How would businesses demonstrate to the Agency that their summaries are complete and accurate reflections of their compliance with CCPA's risk assessment requirements (e.g., summaries signed under penalty of perjury)?**

7. Should the compliance requirements for risk assessments or cybersecurity audits be different for businesses that have less than \$25 million in annual gross revenues? If so, why, and how?

There could be a threshold in which a business can self attest versus a threshold in which a business should be required to have an independent party review the risk assessment. However, it's unclear that gross revenue is the best attribute to qualify a threshold. The problem is, someone could offer a

completely free service (with no income, or minimal income) that poses significant risks to consumers. One modern side effect of a connected society is the ability to crowdsource and turn the labor of consumers into a service for other consumers, with the service provider only providing a platform and skimming income off the top. Millions of hours of content get uploaded by unpaid “content creators” to YouTube every year. Only a few can monetize their creations, but work of those unpaid laborers provides Alphabet a service to its billions of customers. Even a lowly message board, relies on the activities of it’s members to be an attractant to other participants and readers. This is the network effect, the more active members posting, the more attractive it is for readers (whether actively posting or not). A message board need not make much money (and the overhead is low) but the potential for privacy violations is astronomical. One might even conclude that a free or cheap message board (way under the income threshold) lacks the resources to prevent doxing, posting of privacy invasive imagery and videos, or other potential privacy activities. They should be held to account if their service is “likely” to attract posters conducting privacy invasive activities (e.g. a message board dedicated to outing gay politicians versus a message board dedicated to knitters).

8. What else should the Agency consider in drafting its regulations for risk assessments?

Sincerely,

R. Jason Cronk

Enterprivacy Consulting Group

From: Taylor Roschen [REDACTED]
Sent: Wednesday, March 29, 2023 9:10 PM
To: Regulations
Cc: Leticia Garcia
Subject: PR 02-2023
Attachments: CCPA Comment Letter.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please see the attached preliminary comments on behalf of the CA Grocers Association on proposed rulemaking relate to Cybersecurity Audits, Risk Assessments, and Automated Decision making.

Thank you,
Taylor



KAHN, SOARES & CONWAY, LLP

Taylor Roschen
1415 L Street, Suite 400
Sacramento, CA 95814
Office: [REDACTED]
Cell: [REDACTED]

March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: Preliminary Comment on Proposed Rulemaking--
Cybersecurity Audits, Risk Assessments and
Automated Decision Making

Submitted via electronic mail

Honorable Board Members:

The following comments are submitted by the California Grocers Association regarding the preliminary rulemaking process for the California Privacy Rights Act (CPRA) and California Consumer Privacy Act (CCPA) regarding cybersecurity audits, risk assessments and automated decision making. The California Grocers Association (CGA) is a nonprofit statewide trade association representing over 300 retailers operating 6,000 brick and mortar stores and 150 grocery supply companies. We offer these preliminary responses on behalf of our broad membership and in consideration of subsequent impacts.

I. Cybersecurity Audits

With respect to cybersecurity audits, state laws, such as those implemented by the New York Department of Financial Services, allow businesses to submit an annual self-certification to satisfy annual audit requirements. CGA would encourage the Agency to consider a similar allowance. This could be accomplished by providing businesses with the option to provide proof of certification (such as PCI, NIST, or ISO) that demonstrates compliance with audit requirement. We also believe that should “significant risks,” as defined in the CPRA regulations be identified and audit is obligated (e.g. PCI or SOX), these audits should suffice for the CCPA regulations.

On their own accord, many businesses may already perform certain industry standard audits and reports. Some businesses have internal teams that exist solely to conduct audits and that are separate from the first-line teams that are actually implementing security controls. Such an audit can be conducted by auditors internal or external to the covered entity and its affiliates. These teams are designed to be thorough and independent. Businesses should be able to leverage those existing processes to meet CPRA requirements. For example, storage of payment cards on file is regulated by the Payment Card Industry Data Security Standards and merchants are required to re-certify annually. In those circumstances, businesses should be able to re-use such audits/certifications rather than duplicate their efforts, adding undue costs and burdens of compliance to businesses. Likewise, other service providers offer risk assessments, certifications, audits to help meet cybersecurity needs that conform to the obligation in the CCPA. CGA

suggests that the Agency should rely on reasonable industry standards, which include an internal review to ensure independence of the service provider, and not obligate third party auditors, to monitor audit compliance. Particularly with respect to third-party auditors, this may paradoxically present a security risk, as they may expose a business's confidential security practices and potentially underlying data to one or more third parties. This would have an antithetical outcome to the intent of CCPA.

Also, within the scope of cybersecurity audits, CGA implores the Agency to clearly define what types of processing creates a significant risks, and preferably limit the types of information to which the audit applies. This limitation is application is consistent with other audit requirements of personal information, such as payment data. For large businesses, conducting an audit on lower risk personal information that is not obligated in other audits or laws, would create significant expense with no discernable benefit to consumers.

II. Risk Assessments

Significant Risk Definition

CGA recognizes the requirements of the CCPA for the Agency to promulgate regulations for businesses that process consumers' personal information that "presents significant risk to consumers' privacy or security." In determining what type of information and level of processing would be considered "significant," risk assessments should be limited to processing that has a legal or similarly significant effect on the individual, wherein which the information materially affects a decision that will impact housing, education, employment and other areas under the law. It should also be limited to those data points that, if compromised, would result in real, concrete harm to individuals, such as identify theft, extortion or physical injury from intimate partner violence. Additional data measures, such as pseudonymizing or encrypting data can meaningfully reduce risk. Significant risk should not include incidental data processing where that data is not a primary factor, or where the processing of personal information is necessary for fraud prevention, anti-money laundering, or other processes that are legally obligated. These activities protect consumers' privacy and security.

DPIA Content and Assessment Conformance

With respect to the specific content of the DPIA, it should be specific enough for the business and regulator to appreciate the risk, but not be overly prescriptive. This will allow businesses to retain flexibility and scale the existing process to apply a wide variety of factors. We encourage the Agency to consider a similar approach as proposed in the European Union's Article 29 Data Protection Working Group Report from 2017.¹ Moreover, the DPIA and its content should be reviewed for documentation-only purposes; it should not result in the obligation for companies to mitigate or fix identified risks. Finally, the Agency should permit a single risk assessment to satisfy multiple, related types of data processing activities.

¹ "The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them."

Risk assessments are an increasingly common requirement on state, federal and international data protection and privacy laws. To promote the interoperability, reduce redundancies and minimize impacts on covered businesses, the regulation should specify that the Agency will accept risk assessments required under comparable legal requirements. A consistent standard with clear guidelines would allow businesses to continue to build robust systems to protect consumers information, innovate data protection assessments and accurately assess cybersecurity risks. To that end, we encourage the Agency to align the data impact and risk assessment obligations of the CCPA with other similar laws, such as CPA and VCDPA, as a starting point. This is caveated in that the Agency should not adopt, in full, any future regulatory guidance under those laws, including GDPR. Case law is an evolving process and California's obligations should be led and practicable for California businesses.

Methods of Submission

As a threshold matter, the Agency should clarify that its function under the CCPA is to provide "a public report summarizing the risk assessments filed with the Agency." It does however, incorrectly refer to the risk assessment identified in 1798.185(15)(a) rather than 1798.185(15)(b). DPIA summaries should highlight the most significant privacy risks associated with data processing and steps taken to mitigate that risk. They should include commercially sensitive or proprietary data, or security information, such as technical safeguards that could be used to compromise security practices. CGA encourages the Agency to not be overly prescriptive about the manner of risk assessment submission to allow businesses to retain flexibility to repurpose risk assessments in a manner that meets California's content requirements. We also encourage the Agency to consider the submission of risk assessments for processing activities to only be obligated when there is a material change that may pose a new or highlighted risk. If the Agency would prefer a time structured periodic update, absent changes, we encourage consideration of once every three years.

Other Considerations

When balancing risks and benefits, the regulations should consider the reasonable expectations of customers, processing and the relationship between the consumer and business, and any technical or organizational measures and safeguards implemented to mitigate risks. The regulations should also provide businesses with confidence that the risk assessments will not be used to invite future litigation or as evidence in penalty procedures and therefore, all risk assessments conducted under CPRA should be confidential and not subject to the California Public Records Act and note explicitly that submission of an assessment is not a waiver of attorney-client privilege or work product protection.

III. Automated Decision Making

When considering automated decision making, the Agency should bear in mind the following context: automation is a set of decision making and so existing laws that govern how a business makes decisions generally would also apply to automated decision making (ADM).

Existing Standards

As is the case for risk assessment protocols, companies in the United States are subject to several existing (or enacted but not yet in effect) privacy laws that already impose a substantial

obligation on companies that offer the consumer right to opt out of automated decision making.² For interoperability, the Agency should confirm that profiling opt out (1) only applies to decisions with “legal and similarly significant effect;” (2) is limited to solely or fully automated decisions; and (3) applies only after an automated decision is made. The following contains more specific descriptions of CGA’s recommendations on these items:

(1) The Agency should not regulate low risk automated systems (such as spell check, translation, etc.) which would slow down activity substantially and provide no consumer benefit. Rather, the Agency should focus on high risk use cases that would meet our proposed definition of significant risk. For example, under Virginia’s privacy law, the consumer’s right to opt out of profiling is restricted to “decisions that produce legal or similarly significant effects concerning a consumer,” which includes impacts on financial and lending services, housing, insurance, educational enrollment, criminal justice, employment opportunities, health care or access to basic necessities.

(2) Focusing on solely or fully automated decisions avoids creating unreasonable obligations on businesses, without impacting a consumer’s right to have their decisions accessed by a human.

(3) Automation is one way in which companies can manage making multiple decisions daily and provide faster, more predictable customer service and experiences. Forcing companies to have the option of human involvement before decisions are made would be a significant burden on companies, who may be able to support the same number of requests without incurring unreasonable expense.³ In addition to slowing service and increasing costs, a pre-decisional requirement would not provide consumers with a discernible benefit. For example, if an individual applies for a loan and have a positive outcome on the first automated decision, which will likely not want or need to opt out and request review, but would still be entitled to. If they had a negative outcome, they will still be able to exercise their right to contest and have a human issue a new decision. If regulations force companies to have the opt out even before a decision is made, the experience could take days to process without consumer benefit because it would ultimately have the same outcome as the above prescribed example.

Existing Practices

Practically speaking, companies do not typically have requirements, frameworks, or best practices that address access/opt outs related to low risk, every day technology, even those that arguably make automated decisions. Access or opt out rights for this type of automated decisions would slow down business substantially with no benefit to consumers. For example, businesses do not typically give consumers the right to opt out of using optical character recognition on PDF documents containing that consumer’s personal information. Or, they do not give consumers the

² This includes but is not limited to Colorado, Connecticut, and Virginia state privacy laws.

³ For example, individuals receive faster access to services if businesses can quickly identify low fraud risks, which is only possible with simple algorithms --approve transaction with no prior fraud flags – or more complex algorithms including ones using machine learning. Then, for the smaller set of fraud risk cases, businesses can use manual review to make final decisions, for example through an appeals process. In these situations, if non-final decisions – e.g., cases flagged only by algorithms for further human review – are regulated, then consumers will receive slower access to services, and will incur higher costs from increased, and unnecessary, manual review.

right to opt out of having their information stored in an internal database that automatically sorts information alphabetically, and instead demand handwritten records be stored and sorted manually. Regulations should not dictate how businesses use (or don't use) everyday, low-risk technology. With respect to a definition of "automated decision making technology," to avoid an overly broad definition that captures all technologies and software, the Agency should focus on automatic decision making systems that use ML which produce legal or similarly significant effects. ML generally implicates transparency, bias, and explain-ability considerations.

Therefore, CGA proposes that automated decision-making technology should be defined as:
"final decisions that are made solely/fully with AI/ML technology with legal or similarly significant effects."

AI/ML can be further defined as:

"the use of machine learning and related technologies that use data to train algorithms and predictive models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, natural language processing, and speech recognition."

To comply with GDPR, companies already allow European Union customers to request review of certain fully automated decisions; this service can be extended to U.S. customers, as appropriate.

Business and Consumer ADM Practices

Businesses in every industry sector use ADM to improve their competitiveness and enhance their product and service offerings, including routine and low-risk applications. With respect to AI/ML, it is important to note that the adoption of AI across industries is now so widespread that a 2021 McKinsey and Company study found that 56% of business leaders across the globe now report using AI in at least one business function. The McKinsey report highlights that the most common AI uses cases are low risk, involving service-operations optimization, AI-based enhancement of products, and contact-center automation. Automated technologies, likewise, have significant benefits for consumers, including enhanced accuracy and consistency, safer and more innovative products, scalability, cost saving and increased efficiency. Accordingly, the Agency should be mindful of providing consumers any right to opt out of automated activities, and the impacts to consumers' ability to realize those advantages.

If high risk business offerings are essential or critical, it is not reasonable for consumers to consider other options. Businesses should have the ability to demonstrate compliance with operational guardrails in lieu of providing opt out. These guardrails could include rigorous testing, corroboration of results, system monitoring and an appeals or complaint procedure. Automation may also be core to certain high risk service offerings, making opt out infeasible. For example, an in-car safety system that senses a crash and connects with driver assistance shouldn't be required for the consumer to sort a manual process that conducts the same task. Automation may also be essential for products that involve less significant effects. Calendars that provide updated travel times based on traffic patterns are one example. Businesses shouldn't be obligated to design a worse (an potentially more dangerous) version of products and services merely to give consumers a right to opt out of ADM. The Agency should follow the approach of other states privacy laws and limit profiling opt out to automation that has legal or similarly

significant effects. Finally, some uses of automated decision making that produces legal or similarly significant effects may also be highly beneficial to consumers—reducing risk of potential harm. These could include health care systems that use an individual’s address to determine the closest ambulance dispatch, a bank that uses income or account balances to assess credit, or fraud protection. To protect California consumers’ interests without burdening beneficial uses, the Agency should tailor the scope of “legal or similarly significant effects” to the harms regulators seek to protect against and permit operational guardrails rather than requiring an opt out.

Access Requests

Businesses should be able to fulfill consumer access requests by providing a general explanation of technology functionality, rather than information on specific decisions made, via publicly available disclosures on their webpages. Satisfying the “meaningful” information standard, 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 and could conflict with the intellectual property, trade secret, and other legal rights of the business in question. As noted previously with respect to risk assessment, any regulation should 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.

Other Considerations

Businesses should be allowed to use race/ethnicity and other demographic data with the user’s consent for the narrow purpose of evaluating and preventing bias. Regulators should consider a safe harbor for businesses that are trying to prevent bias.

Regarding the Employee and Business-to-Business data, the profiling opt out should exclude automation involving individual data in the employment or and commercial contexts. With respect to the employment context:

- (1) There are developing state and local laws that already specifically target the use of these technologies in the workplace, so California should let that regulatory activity run its course;
- (2) Those laws are being tailored to the nuances of an employment context and, recognizing the potential unreasonableness of requiring specific opt-outs for every instance of automated decision-making, are mainly focused on transparency and human review;
- (3) Basically any decision in the employment context arguably could have a “legal or similarly significant effect,” including innocuous ADM like task allocation that is intended to enable efficiency and scale.

Any regulations around automated decision making require necessary exceptions to access/opt out to avoid abuse (as is already the case in other states). These exemptions should include, in a non-exhaustive format:

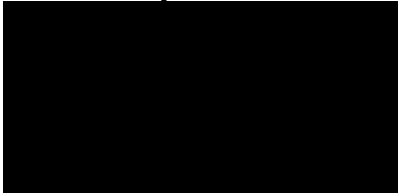
- Prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the

integrity or security of systems or investigate, report or prosecute those responsible for any such action.

- Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by authorities.
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may be illegal.
- Provide a product or service a consumer requested or perform a contract with the consumer.
- Take immediate steps to protect an interest that is essential for the life of the consumer or another natural person, if the processing cannot be manifestly based on another legal basis.
- Process personal data for reasons of public interest in the area of public health, subject to certain conditions.
- Conduct internal research.
- Fix technical errors.
- Perform internal operations that are consistent with the consumer's expectations.

We would like to thank you for the opportunity to provide preliminary comments and would welcome any further discussion with you and your staff as this regulatory package moves forward.

Sincerely,



Leticia Garcia, Director
State Government Relations
California Grocers Association

From: Joanne Furtsch [REDACTED]
Sent: Monday, May 8, 2023 2:48 PM
To: Regulations
Cc: Andrew Scott
Subject: Re: CPPA Public Comment: PR 02-2023
Attachments: CCPA Regulation Comments Round 2 FINAL.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attn: Kevin Sabo

It has come to my attention that the incorrect version of TrustArc's comments were submitted as part of our original submission on March 27, 2023. Please find the correct version of TrustArc's comments regarding the proposed rulemaking for cybersecurity audits, risk assessments, and automated decision making attached. Contact me if you have any questions.

Best -
Joanne Furtsch

On Mon, Mar 27, 2023 at 8:34 AM Joanne Furtsch [REDACTED] wrote:
Attn: Kevin Sabo

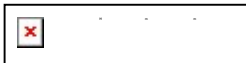
Please find TrustArc's comments regarding the proposed rulemaking for cybersecurity audits, risk assessments, and automated decision making attached. Contact me if you have any questions.

Best -
Joanne Furtsch

Joanne B. Furtsch

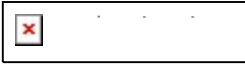
Director, Privacy Intelligence Development / CIPP/US/C, CIPT, FIP

M: [REDACTED] | [REDACTED]



CONFIDENTIALITY NOTICE: This email including any attachments, may contain information that is confidential. Any unauthorized disclosure, copying or use of this email is prohibited. If you are not the intended recipient, please notify us by reply email or telephone call and permanently delete this email and any copies immediately.

--



Joanne B. Furtsch

Director, Privacy Intelligence Development / CIPP/US/C, CIPT, FIP

M: [REDACTED] | [REDACTED]

CONFIDENTIALITY NOTICE: This email including any attachments, may contain information that is confidential. Any unauthorized disclosure, copying or use of this email is prohibited. If you are not the intended recipient, please notify us by reply email or telephone call and permanently delete this email and any copies immediately.

March 27, 2023

California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834
Attn: Kevin Sabo

By Email Submission to: regulations@coppa.ca.gov

RE: TrustArc's CCPA Proposed Rulemaking Public Comment

TrustArc Inc ("TrustArc") appreciates the opportunity to provide comments on the proposed rulemaking for cybersecurity audits, risk assessments, and automated decision making. We understand the importance of risk assessments to help organizations effectively identify where they have data processing risks so they can address those risks and protect consumers from data processing harms. We feel our experience in helping organizations develop risk assessments and workflows to manage the assessment process will help inform the Agency's rulemaking.

Our comments center around the approach to risk assessments and its benefits and drawbacks, what content needs to be included in the assessments, when they should be submitted to the Agency, and who should need to complete them.

We want to emphasize the following:

- Prescriptive requirements in performing risk assessments and possible burdensome reporting requirements means businesses will lose efficiency. This will place strains on internal business processes and relationships between privacy teams and their business stakeholders.
- The process and workflow for completing risk assessments varies across organizations and it is important to give organizations flexibility in structuring their risk assessments providing that the content requirements are met.
- Organizations should only be required to submit their annual risk assessments to the Agency upon request as part of its cooperation in an investigation initiated by the Agency.
- The rulemaking for risk assessments needs to be clear at what level the risk assessment needs to be conducted whether it is at the organizational level or the business processing activity level.
- The requirement to complete risk assessments should be based on the organization's data processing risk, not the organization's size or annual revenue.

Our detailed comments are provided below. For any questions regarding this submission, please contact Joanne Furtsch, Director, Privacy Intelligence Development, at [REDACTED].

CPPA Question #3: The EDPB's Approach to Data Protection Impact Assessments

3. To determine what processing of personal information presents significant risk to consumers' privacy or security under Civil Code § 1798.185(a)(15):

- a. What would the benefits and drawbacks be of the Agency following the approach outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessment?
- b. What other models or factors should the Agency consider? Why? How?
- c. Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? Why, or why not? If so, how?
- d. What processing, if any, does not present significant risk to consumers' privacy or security? Why?

The EDPB's Approach to DPIAs

Article 35 of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or "GDPR")¹ provides:

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. ...
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
 - a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
 - b. processing on a large scale of special categories of data ..., or of personal data relating to criminal convictions and offenses ...; or
 - c. a systematic monitoring of a publicly accessible area on a large scale.
4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.
5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

In October 2017, the Article 29 Data Protection Working Party, as the European Data Protection Board (EDPB) was known at the time, issued Working Paper 248², Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of

¹ Official legal text of GDPR: <https://gdpr-info.eu/>

² Working Paper 248: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711

Regulation 2016/679. These guidelines established guidance on which processing operations are likely to result in a high risk to the rights and freedoms of natural persons, and therefore subject to a DPIA.

In the Guidelines, the EDPB took a broad and non-exhaustive approach, leaving it to the national supervisory authorities to be more explicit. The EDPB noted that not only the risk to the right of data protection and privacy may be implicated, but also the impact of processing on other fundamental freedoms must be considered: freedom of speech; freedom of thought; freedom of movement; prohibition of discrimination; and right to liberty, conscience and religion.

The following criteria were presented to help determine if a high risk to the rights and freedoms of natural persons is likely. If more than one of these criteria is present, then a DPIA is presumed to be necessary; failure to conduct a DPIA where more than one of these criteria is present must be documented along with the rationale for why it does not reflect a high risk. The criteria listed are:

1. Evaluation or scoring, including profiling and predicting, especially from “aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements”.
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing “legal effects concerning the natural person” or which “similarly significantly affects the natural person”. For example, the processing may lead to the exclusion or discrimination against individuals.
3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or “a systematic monitoring of a publicly accessible area”. The personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used, and it may be impossible for individuals to avoid being subject to such processing.
4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 of the GDPR, personal data relating to criminal convictions or offences, as well as categories of data considered as increasing the possible risk to the rights and freedoms of individuals: because they are linked to household and private activities (such as electronic communications), because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement), or because their violation clearly involves serious impacts in the data subject’s daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant.
5. Data processed on a large scale: this is not defined but the following factors can be considered in determining a large scale:
 - a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
 - b. the volume of data and/or the range of different data items being processed;
 - c. the duration, or permanence, of the data processing activity;
 - d. the geographical extent of the processing activity.
6. Matching or combining datasets, originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

7. Data concerning vulnerable data subjects: the increased power imbalance between the data subjects and the data controller means that individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children, employees, and more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, the elderly, patients, etc.).
8. Innovative use or applying new technological or organizational solutions. This can involve novel forms of data collection and usage, and the personal and social consequences of the deployment of a new technology may be unknown.
9. When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”. This includes processing operations that aim at allowing, modifying or refusing data subjects’ access to a service or entry into a contract.

Benefits and Drawbacks of the EDPB Approach

There are a number of benefits the Agency could achieve by adopting this approach to determining when risk assessments must be carried out:

- Processing around data aggregation; automated decisions and algorithms; and monitoring or profiling, remains opaque to consumers and pose a higher risk to consumers’ rights and freedoms, such that these types of activities should be factored into the risk threshold.
- For businesses already subject to the GDPR, they would be able to take advantage of existing processes and benefit from consistency in policy.
- The European Union is thought of as a global leader in privacy protection, and by adopting a similar approach, California companies who sell to European markets could use their risk assessments as a way of demonstrating to their customer base a strong adherence to European privacy norms, as well as position their offering using privacy as a differentiator.
- The EDPB stated that when in doubt about whether processing is likely to result in a high risk, it should be resolved in favor of performing a DPIA. This approach puts consumers first and focuses on guaranteeing all of their rights and freedoms, beyond privacy.
- There are some pragmatic elements in the GDPR and the EDPB’s approach that should be adopted:
 - Only a single assessment is necessary for similar processing operations.
 - Assessments do not need to be repeated where they have already been performed; however, the data controller must continue to review whether there are any changes to processing that necessitate a DPIA.

The EDPB’s approach is not without its drawbacks. First, the meaning of “large scale” should be clarified to help organizations better understand when that threshold has been crossed:

1. The aspects related to volumes need defined ranges to provide necessary clarity. Processing should be considered as presenting a higher risk when:
 - More than 100,000 consumers’ personal information is captured; and
 - More than 100,000 records of personal data are captured.
2. The factor relating to duration or permanence of processing should be expanded upon. One possibility is to align with other timeframes in the CCPA. If the default entitlement for consumers is to an accounting of sales and sharing of personal information in the past year, then the factor related to duration should be similarly defined: processing that takes place over a period of more than one year would possibly pose a higher risk.

3. The factor relating to geographic extent of processing should be replaced with consideration of data transfers to third countries that lack adequate protection for the personal information. For example, a business that processes personal information across the entirety of the United States may have a smaller degree of risk than a business that processes only personal information of Californians but sends that personal information to countries like Russia, the People's Republic of China or other countries with known privacy-invasive regimes.

In the lists published by national supervisory authorities of when a DPIA is required, a number of them called out certain industries as requiring to conduct a DPIA regardless of their processing purposes, due to the nature of the information they hold (Finance, Healthcare) or scale of operations (Telecommunications). The Agency is urged to not make industry alone a determinative factor in when a DPIA is required. These industries engage in many practices that are long standing and in line with the reasonable expectations of consumers, such that they do not by virtue of industry alone, pose a higher risk to the risks and freedoms of consumers.

Finally, if the Agency adopts the EDPB's approach, the Agency is urged to consider that very prescriptive requirements in performing the DPIA and the possible burdensome reporting means that businesses lose efficiency. This may be detrimental to the relationship between internal privacy teams and their business stakeholders, as such cumbersome processes may create a deterrence in business stakeholders accurately reporting their activities to the privacy team.

Additional Factors or Models to Consider

The approach that the Agency adopts should focus on harm reduction: processing where there is a lack of transparency and choice, and little recourse for individuals. The model should be tailored to consider who is involved in the processing (are there vulnerable populations involved or power imbalances at work), what is involved in the processing (the degree of sensitivity of the personal information), and what is the understanding of what is going to happen, or in other words, what are the reasonable expectations of the consumer.

While a cybersecurity audit should be conducted where there is a need to protect the confidentiality, integrity and availability of personal information against the ongoing risks posed by malicious third parties and insider threats, a PIA on the other hand should focus on minimizing the invasion of privacy on consumers prior to the initiation of processing. In this, the Agency should allow for the possibility of industry association-lead PIAs, and allow vendors to conduct a PIA on their tool, software, technology, which can be relied upon by the businesses that are members of that industry or purchase that vendor's goods or services.

With respect to processing activities that do not present a significant risk to consumer privacy, for which a PIA is not required. A starting point could include:

- Where processing involves only publicly available information or information akin to directory type elements (name, telephone number);
- Processing required by law;
- Processing involving business to business relationships;
- Processing that strictly adheres to a recognized code of conduct; and
- Processing where a PIA has already been completed, e.g., by an industry association or vendor.

CPPA Question #4: Assessment Content Considerations

4. *What minimum content should be required in businesses' risk assessments? In addition:*
- a. *What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act?*
 - b. *What, if any, additional content should be included in risk assessments for processing that involves automated decision making, including profiling? Why?*

Risk Assessment Content

TrustArc takes a holistic approach to designing its risk assessments, factoring in requirements of multiple jurisdictions to harmonize the questions. The goal in doing this is to help organizations have a simple workflow for getting the assessments completed and to reduce the number of assessments that need to be completed. Organizations with small privacy teams rely on the business owners to complete the assessments for the systems or business process activities they are responsible for. It is challenging to get business owners to complete one assessment let alone multiple assessments which is another key reason why we took a holistic approach to developing the assessment content.

At a minimum, TrustArc risk assessments contain questions around the controls an organization has in place for the following risk areas:

- Data Minimization - assessing that the appropriate controls are in place to minimize data storage related risks and that only the minimum amount of data needed and relevant to the business processing activity is collected.
- Use, Retention, and Disposal - determining whether the use of data is limited to purposes for which it was collected, that is processed for purposes allowed under applicable laws, and retention periods and disposal methods have been defined.
- Disclosure to Third Parties - verifying that third party recipients of data have been assessed to determine if they have appropriate controls to protect the data they receive, and that required contracts are in place.
- Choice and Consent - assessing whether required mechanisms to obtain the consumer's consent where required and provide consumers choice and the ability to opt-out have been properly implemented including whether evidence of the consumer's choice is maintained and that the consumer knows they can opt-out at any time.
- Individual Rights - covering whether the required mechanisms and processes necessary for the consumer to exercise their rights are in place. This includes rights relating to the automated processing of consumer information.
- Data Quality and Integrity - determining whether mechanisms to ensure data is up to date, accurate, and timely for the business processing activity are in place.
- Security - determining whether the appropriate organizational, contractual and technical safeguards based on the level of sensitivity of the data and the means and purposes of processing are in place.
- Transparency - ensuring requirements to inform consumers about the processing of their data are met including timing and placement of consumer notices.

The risk assessment needs to be comprehensive and the risk areas listed above are the minimum TrustArc recommends that should be included in a risk assessment. Questions should be required based on the organization's practices related to the business processing activity. Organizations should only have to answer the questions that are applicable to that specific activity. For example, if the organization does not offer financial incentives, they should not be required to answer questions about financial incentives.

The rules relating to risk assessments need to be clear at what level the risk assessment needs to be conducted: whether it is at the organizational level or at a business processing activity level. This will dictate the number of assessments the organization will need to complete. Risk assessments are typically conducted at the business processing activity level.

Harmonization of Assessment Content

As noted above, TrustArc believes a harmonized and holistic approach to risk assessment content requirements will benefit businesses in having to complete one assessment that will satisfy the requirements across multiple jurisdictions. This is especially important for small businesses with limited resources. This will reduce the costs to businesses and reduce strain between privacy teams and their internal business stakeholders by not having to complete multiple assessments, especially where there is overlap between requirements across different jurisdictions.

Also, businesses should be able to combine the risk assessment content as required in the CCPA regulations with content required by other jurisdictions so they can develop a single risk assessment template. The process and workflow for completing risk assessments varies across organizations and it is important to give organizations flexibility in structuring their risk assessments providing the content requirements are met. TrustArc knows this from its experience in working with hundreds of its customers to set up their risk assessment workflows in TrustArc's Risk Profile³ application.

Assessing Processes Involving Automated Decision Making

TrustArc agrees additional question content should be required relating to processing that involves automated decision making, including profiling because this type of processing presents the greatest risk of harm to consumers, especially in the event of a negative decision.

TrustArc's risk assessments include questions to help organizations determine if the appropriate controls to manage risk around automated decisioning are appropriate. Both GDPR and China's PIPL require organizations to assess their practices around automated decision making. It is important to understand whether the process is transparent to consumers, if the consumer can request a human review in the event that a negative decision having significant legal and life implications was solely based on automated decisioning, what type of notification the consumer receives regarding the negative decision and their rights around contesting it, and what controls are in place to ensure biases are removed from the decision-making algorithm. The questions should only be required if the organization engages in this type of practice.

³ <https://trustarc.com/risk-profile/>

CPPA Question #6: Assessment Submission Format

6. *In what format should businesses submit risk assessments to the Agency? In particular:*
- b. How would businesses demonstrate to the Agency that their summaries are complete and accurate reflections of their compliance with CCPA's risk assessment requirements (e.g., summaries signed under penalty of perjury)?*

Assessment Submission

Organizations should submit risk assessments to the Agency only as part of responding to a compliance investigation initiated by the Agency if the organization needs to demonstrate they have completed the assessments. Organizations need to complete their assessments at least annually or if there is a change to the business processing activity, and should be able to provide them to the Agency upon request.

Requiring organizations to submit their assessments or summaries of their assessments to the Agency annually adds an additional reporting cost for organizations, especially small businesses. Also, requiring assessments or summaries to be submitted does not provide any additional protections or benefits to California consumers.

Organizations should be able to submit the requested assessments or audits electronically whether it is sent via email or uploaded onto a website or cloud application. The Agency should accept common file formats such as .csv, .pdf, .xlsx, .docx.

Attestations Regarding Accuracy of Assessment Responses

As part of its assessments for its Assurance Programs, TrustArc requires program participants to attest that they are authorized to submit the assessment and attest to the accuracy of the information provided in response to the questions. A simple attestation to the accuracy of the responses should be sufficient as the CCPA as amended by CPRA gives the Agency enforcement powers to address violations of the law. As noted above, the assessments or audit results should only be provided to the Agency upon request as needed to conduct investigations into non-compliance with the law.

CPPA Question #7: Different Assessment Requirements Based on Annual Revenue

7. *Should the compliance requirements for risk assessments or cybersecurity audits be different for businesses that have less than \$25 million in annual gross revenues? If so, why, and how?*

Risk-based Approach to Requiring Assessments

No. Compliance requirements for risk assessments or cybersecurity audits should not be different for businesses with less than \$25 million in annual gross revenues. The compliance requirements for risk assessments and cybersecurity audits should be risk or harm based, focusing on the types of business

processing activities the organization is engaged in, the types of data involved, the types of individuals whose data is involved in the processing, and the volume of data being processed.

Revenue is not a measure for risk.

As noted in our response to Question 3, the benefit of taking a risk based approach to when a risk assessment is required will provide a level of greater protection for California consumers by putting consumers first and focusing on guaranteeing all of their rights and freedoms, beyond privacy. This ensures that organizations engaging in high risk data processing activities will be able to demonstrate what protections are in place and be held accountable for any misuse.