CALIFORNIA PRIVACY PROTECTION AGENCY
2101 Arena Blvd
Sacramento, CA 95834
www.cppa.ca.gov

DISCUSSION DRAFT FOR FEBRUARY 3, 2023 CPPA BOARD MEETING

INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING

Background

In November of 2020, voters approved Proposition 24, the California Privacy Rights Act of 2020 ("CPRA"). The CPRA amends and extends the California Consumer Privacy Act of 2018 ("CCPA"). To implement the law, the CPRA established the California Privacy Protection Agency ("Agency") and vested it with the "full administrative power, authority and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018,"[1] including the authority to promulgate regulations.[2] As part of its rulemaking responsibilities, the Agency is directed to do the following pursuant to Civil Code section 1798.185(a)(15)-(16):

> (15) Issu[e] regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:
>
> (A) Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.
>
> (B) Submit to the California Privacy Protection Agency on a regular basis 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 resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.
>
> (16) Issu[e] regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.

[1] Civil Code, § 1798.199.10(a).
[2] See Civil Code §§ 1798.185(d), 1798.199.40(b).

Invitation for Comments

In accordance with Government Code sections 11346, subdivision (b), and 11346.45, the Agency seeks input from stakeholders in developing regulations that implement the abovementioned statutory provisions. **PLEASE NOTE: The public is invited to submit comments specifically relating to cybersecurity audits, risk assessments, and automated decisionmaking.** The Agency is particularly interested in receiving views and comments on the topics and questions provided below. However, stakeholders are not limited to providing comments in the areas identified by the Agency and may comment on any potential area for rulemaking within the scope of Civil Code section 1798.185(a)(15)-(16). The tenor and substance of the topics and questions should not be taken as an indication that the Agency is predisposed to any particular views, positions, or actions. Comments will assist the Agency in developing new regulations that implement the law in the most effective manner. The Agency invites stakeholders to propose specific language for new regulations that implement, interpret, or make specific Civil Code section 1798.185(a)(15)-(16). Commenters are encouraged to review the short "Tips for Submitting Effective Comments" guide[3] for help formulating and submitting effective comments. This invitation for comments is not a proposed rulemaking action under Government Code section 11346. This invitation for comments is part of the Agency's preliminary rulemaking activities under Government Code section 11346, subdivision (b). The public will have the opportunity to provide additional comments on any proposed regulations when the Agency proceeds with a notice of proposed rulemaking action. All terms used in this Invitation for Comments are as defined in the CCPA, as amended by the CPRA, and the CCPA regulations.[4]

Topics for Public Comment

Below, the Agency has formulated topics and questions to assist interested parties in providing input on rulemaking.

I. Cybersecurity Audits

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 perform annual cybersecurity audits, "including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent."[5] In determining the necessary scope and process for these audits, the Agency is interested in learning more about existing state, federal, and international laws applicable to some or all CCPA-covered businesses or organizations that presently require some form of cybersecurity audit related to the entity's processing of consumers' personal information; other cybersecurity audits, assessments, or evaluations that are currently performed, and cybersecurity best practices; and businesses' relevant compliance processes. Accordingly, the Agency asks:

[3] Available at https://cppa.ca.gov/regulations/pdf/comments_tips.pdf.
[4] See Code Regs., tit. 11, § 7000, et seq.
[5] Civil Code § 1798.185(a)(15)(A).

1. What laws that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require cybersecurity audits? For the laws identified:

    a. To what degree are these laws' cybersecurity audit requirements aligned with the processes and goals articulated in Civil Code section 1798.185(a)(15)(A)?
    b. What processes have businesses or organizations implemented to comply with these laws that could also assist with their compliance with CCPA's cybersecurity audit requirements?
    c. What gaps or weaknesses exist in these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?
    d. What gaps or weaknesses exist in businesses' compliance processes with these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?
    e. Would you recommend that the Agency consider the cybersecurity audit models created by these laws when drafting its regulations? Why, or why not?

2. In addition to any legally-required cybersecurity audits identified in response to question 1, what other cybersecurity audits, assessments, or evaluations that are currently performed, or best practices, should the Agency consider in its regulations for CCPA's cybersecurity audits pursuant to Civ. Code § 1798.185(a)(15)(A)? For the cybersecurity audits, assessments, evaluations, or best practices identified:

    a. To what degree are these cybersecurity audits, assessments, evaluations, or best practices aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(A)?
    b. What processes have businesses or organizations implemented to complete or comply with these cybersecurity audits, assessments, evaluations, or best practices that could also assist with compliance with CCPA's cybersecurity audit requirements?
    c. What gaps or weaknesses exist in these cybersecurity audits, assessments, evaluations, or best practices? What is the impact of these gaps or weaknesses on consumers?
    d. What gaps or weaknesses exist in businesses or organizations' completion of or compliance processes with these cybersecurity audits, assessments, evaluations, or best practices? What is the impact of these gaps or weaknesses on consumers?
    e. Would you recommend that the Agency consider these cybersecurity audit models, assessments, evaluations, or best practices when drafting its regulations? Why, or why not? If so, how?

3. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted cybersecurity audits that the business completed to comply with the laws identified in question 1, or if the Agency accepted any of the other cybersecurity audits, assessments, or evaluations identified in question 2? How would businesses demonstrate to the Agency

that such cybersecurity audits, assessments, or evaluations comply with CCPA's cybersecurity audit requirements?

4. With respect to the laws, cybersecurity audits, assessments, or evaluations identified in response to questions 1 and/or 2, what processes help to ensure that these audits, assessments, or evaluations are thorough and independent? What else should the Agency consider to ensure that cybersecurity audits will be thorough and independent?

5. What else should the Agency consider to define the scope of cybersecurity audits?

II. Risk Assessments

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.[6] 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 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? 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)?
    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)?
    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?
    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?

[6] Civil Code § 1798.185(a)(15)(B).

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?

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?

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?

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 decisionmaking, 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?

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

III. Automated Decisionmaking

The CCPA directs the Agency to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decision making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision making processes, as well as a description of the likely outcome of the process with respect to the consumer."[7] In determining the necessary scope of such regulations, the Agency is interested in learning more about existing state, federal, and international laws, other requirements, frameworks, and/or best practices applicable to some or all CCPA-covered businesses or organizations that presently utilize any form of automated decisionmaking technology in relation to consumers, as well as businesses' compliance processes with these laws, requirements, frameworks, and/or best practices. In addition, the Agency is interested in learning more about businesses' uses of and consumers' experiences with these technologies, including the prevalence of algorithmic discrimination. Lastly, the Agency is interested in the public's recommendations regarding whether access and opt-out rights should differ based on various factors, and how to ensure that access requests provide meaningful information about the logic involved in automated decisionmaking processes as well as a description of the likely outcome of the process with respect to the consumer. Accordingly, the Agency asks:

1. What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?

2. What other requirements, frameworks, and/or best practices that address access and/or opt-out rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?

3. With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:

    a. How is "automated decisionmaking technology" defined? Should the Agency adopt any of these definitions? Why, or why not?

[7] Civil Code § 1798.185(a)(16).

b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the requirements, processes, and goals articulated in Civil Code § 1798.185(a)(16)?
c. What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA's automated decisionmaking technology requirements?
d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?
e. What gaps or weaknesses exist in businesses or organizations' compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?
f. Would you recommend that the Agency consider these laws, other requirements, frameworks, or best practices when drafting its regulations? Why, or why not? If so, how?

4. How have businesses or organizations been using automated decisionmaking technologies, including algorithms? In what contexts are they deploying them? Please provide specific examples, studies, cases, data, or other evidence of such uses when responding to this question, if possible.

5. What experiences have consumers had with automated decisionmaking technology, including algorithms? What particular concerns do consumers have about their use of businesses' automated decisionmaking technology? Please provide specific examples, studies, cases, data, or other evidence of such experiences or uses when responding to this question, if possible.

6. How prevalent is algorithmic discrimination based upon classifications/classes protected under California or federal law (e.g., race, sex, and age)? Is such discrimination more pronounced in some sectors than others? If so, which ones? Please provide specific examples, studies, cases, data, or other evidence of such discrimination when responding to this question, if possible.

7. How can access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, address algorithmic discrimination?

8. Should access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, vary depending upon certain factors (*e.g.*, the industry that is using the technology; the technology being used; the type of consumer to whom the technology is being applied; the sensitivity of the personal information being used; and the situation in which the decision is being made, including from the consumer's perspective)? Why, or why not? If they should vary, how so?

9. What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decisionmaking processes and the description of the likely outcome of the process with respect to the consumer? In addition:

    a. What mechanisms or frameworks should the Agency use or require to ensure that truly meaningful information is disclosed?
    b. How can such disclosure requirements be crafted and implemented so as not to reveal a business or organization's trade secrets?

10. To the extent not addressed in your responses to the questions above, what processes should be required for access and opt-out rights? Why?

Time for Comments

The Agency invites interested parties to submit comments by [DATE], 2023.

Where to Submit Comments

You may submit comments by the following means: [Submission information to come.]

Contact Person

Questions regarding this invitation for comments may be directed to [Name, title, contact to come].