STATE OF CALIFORNIA Gavin Newsom, Governor

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

New Rules Subcommittee

Sample Questions for Preliminary Rulemaking

Risk Assessments

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?
   a. To what degree are these risk-assessment requirements aligned with the processes and goals articulated in Civ. 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?
   d. What gaps or weaknesses exist in businesses' or organizations' compliance processes with these laws, other requirements, or best practices for risk assessments?
2. What communities or individuals are more susceptible to harm from a business's data processing practices? Why are they more susceptible to harm from these data processing practices?
3. To determine what processing of personal information presents significant risk to consumers' privacy or security under Civ. 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?
   c. Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? If so, how?
   d. What processing, if any, does not present significant risk to consumers' privacy or security?
4. What minimum content should be required in businesses' risk assessments?
   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?
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. How should businesses submit risk assessments to the Agency?

    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), what should these summaries include?
    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?

Cybersecurity Audits

1. What laws that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require cybersecurity audits?
    a. To what degree are these cybersecurity-audit requirements aligned with the processes and goals articulated in Civ. Code § 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?
    d. What gaps or weaknesses exist in businesses' compliance processes with these laws for cybersecurity audits?
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)?
    a. To what degree are these cybersecurity audits, assessments, evaluations, or best practices aligned with the processes and goals articulated in Civ. 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?
    d. What gaps or weaknesses exist in businesses or organizations' completion of or compliance processes with these cybersecurity audits, assessments, evaluations, or best practices?
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?

Automated Decisionmaking

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?
    b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the processes and goals articulated in Civ. 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?
    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?
4. 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?
5. How can access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, address algorithmic discrimination?
6. Should access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, differ for consumers across industries and technologies? If so, how should they differ, and why?
7. 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?