BSA | The Software Alliance

Submission to California Privacy Protection Agency
Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decision-Making

BSA | The Software Alliance appreciates the opportunity to submit comments in response to the invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA) and the California Consumer Privacy Act (CCPA) regarding cybersecurity audits, risk assessments and automated decision-making. We appreciate the California Privacy Protection Agency's (CPPA's) work to address consumer privacy and its goal of issuing regulations that better protect consumer privacy.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive data — including personal information — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations, and BSA members' business models do not depend on monetizing users' personal information.

Our comments focus on the three topics on which the CPPA seeks input:

1. ***Cybersecurity Audits.*** New regulations are to require annual cybersecurity audits for businesses whose processing presents a "significant risk" to security. We urge the CPPA to allow companies to satisfy this requirement by demonstrating compliance with existing laws or internationally-recognized cybersecurity standards — without creating new audits or assessments. We also encourage the CPPA to define "significant risk" in line with, or by reference to, leading cybersecurity laws, policies and standards.

2. ***Risk Assessments.*** New regulations are to require businesses whose processing of consumers' personal information presents a "significant risk" to consumers' privacy to submit risk assessments to the CPPA. We urge the CPPA to ensure these risk assessments are interoperable with risk assessments conducted under leading global and state privacy laws. We also encourage the agency to define "significant risk" to privacy in line with leading global and state data protection laws and to focus

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

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

on requiring companies to provide assessments upon request, rather than requiring all companies provide assessments to the agency on a standard timeframe.

3. ***Automated Decision-Making.*** New regulations are to address the use of automated decision making in certain circumstances. We support reading this authority in line with the narrow statutory text, to focus the use of automated decision-making technology in the context of the access and opt-out rights already included in the CCPA. If the agency creates a right to opt out of profiling under California law, we encourage the CPPA to ensure that right aligns with similar rights in global privacy laws and in other states, so that California consumers may exercise their rights using established and centralized processes.

I. Cybersecurity Audits

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

BSA recognizes that data security is integral to protecting personal information and privacy. Given the dramatic increase in the cybersecurity laws worldwide, we strongly encourage the CPPA to focus on recognizing compliance by companies with existing cybersecurity laws and standards — without creating any new certification or audit standards.

Question 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 § 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?*

Companies already comply with a significant range of obligations designed to support strong cybersecurity practices. These include not only obligations that are legally required, but an increasing number of compliance assessments and audits that are regularly used across industry sectors even though they are not directly required by legislation. For example, the United States Government requires companies supplying products or services to federal agencies comply with FedRAMP, the US Department of Defense's Cybersecurity Maturity Model Certification (CMMC), the Federal Information Processing Standards, and forthcoming NIST conformity assessments, among other requirements. Internationally, companies often certify compliance to standards based on the Common Criteria, which underpin the Common Criteria Recognition Agreement. In Japan, the Information System Security Management and

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

Assessment Program (ISMAP) applies cybersecurity protections to government cloud services; the United Kingdom, Korea, Singapore, and Australia have similar schemes.

These requirements are part of a rising number of cybersecurity laws globally. In the European Union alone, the Network and Information Security 2 (NIS2) Directive took effect in January, creating new cross-sector cybersecurity requirements.[3] The EU has also adopted new cybersecurity requirements financial services entities (through the Digital Operational Resilience Act) and is proposing additional cybersecurity regulations for products with digital elements (through the Cyber Resilience Act).

In the United States, businesses conduct audits or assessments of their cybersecurity practices to comply with a range of laws including:

- *Sarbanes-Oxley Act (SOX)***,** which requires publicly traded companies to maintain adequate controls, including cybersecurity controls, over their financial reporting;
- *Health Insurance Portability and Accountability Act of 1996 (HIPAA),* which requires organizations that possess patient health information to protect that information;
- *Gramm-Leach-Bliley Act (GLBA),* which requires financial institutions to secure customer information;
- *Federal Acquisition Regulation (FAR),* which require organizations that sell solutions to the US Government to meet baseline cybersecurity practices; and
- *Defense Federal Acquisition Regulations Supplement (DFARS),* which requires organizations in the defense industrial base to meet baseline cybersecurity practices.

In addition to any legal requirements to conduct cybersecurity audits, customers often require their vendors to demonstrate strong cybersecurity practices — creating another layer of certifications and audit requirements. For example, customers frequently require vendors to certify they are compliant with the ISO 27000 series of standards (which govern information security management)[4] and Service Organization Control (SOC) 2 Type 2 requirements (which assess controls related to security, availability, processing integrity, confidentiality, or privacy of information).[5] Companies that offer multiple products may be required to obtain a certification for each product, compounding these requirements.

Organizations have invested heavily in complying with these cybersecurity obligations, but the increasing number and variety of cybersecurity obligations can make it more costly for companies to serve government and private sector organizations, create additional barriers to entry for smaller businesses, and divert resources that would otherwise focus on substantively improving security. As the President's National Security Telecommunications Advisory Committee (NSTAC) draft Strategy for Increasing Trust Report notes:

> Against this backdrop, the number of security requirements and security assurance programs have increased dramatically. This cacophony has a cost. While government Departments and Agencies (hereinafter, "Agencies") and private businesses have long noted a shortage of qualified security personnel, they have nonetheless created an environment in which valuable and limited resources must be spent to comply with overlapping and sometimes redundant or inconsistent regulatory regimes. To create a more meaningful and robust system, the U.S. government must

[3] EU Directive 2022/2555, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.
[4] *See* ISO/IEC 27001 and related standards, *available at* https://www.iso.org/isoiec-27001-information-security.html.
[5] *See* Association of International Certified Professional Accountants, SOC for Service Organizations, *available at* https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.

streamline the way that security requirements are created, strengthen mechanisms for vendors to demonstrate compliance, and provide easier ways for vendors to convey their efforts to concerned parties.[6]

The Biden-Harris Administration expressly supported harmonizing audit requirements in its recently-published National Cybersecurity Strategy. That Strategy encourages regulators to work together to minimize the harms created by duplicative or overly burdensome regulations, after finding that effective regulations minimize cost burden and thereby enable organizations to invest in "building resilience and defending their systems and assets." The Strategy identifies ensuring cybersecurity regulatory frameworks are "harmonized to reduce duplication" and "cognizant of the cost of implementation" as a strategic objective of the Administration.[7] In addition, the Strategy recognizes that "regulators should work to harmonize not only regulations and rules, but also assessments and audits of regulated entities." This latter point — of harmonizing audits — is critical to avoid duplicative requirements for companies subject to cybersecurity regulations.

In other contexts, states including California have recognized the importance of treating companies as compliant with state requirements when they already fulfill similar federal requirements. For example, California participates in the StateRAMP program, which recognizes that companies that have invested in compliance with FedRAMP are compliant with similar obligations at the state level. The same approach is needed here.

Recommendation: The CPPA should allow companies to satisfy any new California requirements by complying with existing cybersecurity laws or standards, through self-attestation or obtaining a recognized certification, which demonstrates the business is managing cybersecurity risks in line with California requirements

Question 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 Civil 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?*

---

[6] *See* Draft NSTAC Strategy Trust Report (Jan. 31, 2023), *available at* https://www.cisa.gov/sites/default/files/202303/Draft%20NSTAC%20Strategy%20for%20Increasing%20Trust%20Report%20% 281-31-23%29_508.pdf.

[7] National Cybersecurity Strategy, Strategic Objective 1.1 (March 2023), *available at* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

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?*

California should not create its own cybersecurity certification or audit standards. Rather, the CPPA should recognize compliance with existing standards and best practices for cybersecurity risk management as meeting any new California requirements.

In addition to the obligations discussed above, the CPPA should recognize that compliance with existing standards and best practices for cybersecurity risk management, including the NIST Cybersecurity Framework and the ISO 27000 family of standards, meet any new California requirements. NIST's Cybersecurity Framework and ISO 27001 are the leading tools for organizations and governments to use in managing cybersecurity-related risks.[8] NIST is also in the process of updating its Cybersecurity Framework, to keep pace with improvements in cybersecurity risk management. Although the Cybersecurity Framework was initially developed with a focus on critical infrastructure, such as transportation and the electric power grid, it has been adopted far more broadly by cross-sector organizations of all sizes and has been embraced by governments and industries worldwide. Likewise, as the leading global standard for information security, ISO 27001 is leveraged widely by organizations of all sizes. The CPPA should recognize compliance with these longstanding and trusted resources.

By recognizing that compliance with existing cybersecurity obligations meets California's requirements, the CPPA can drive investment in strong practices that lead to better outcomes. In contrast, new regulations that create another layer of audit requirements would fragment compliance and divert resources that could otherwise be focused on substantively improving cybersecurity protections. That approach would also make it much more challenging for California companies to expand and compete in the global marketplace because in addition to meeting the CCPA's requirements, they would then have to invest heavily in meeting the cybersecurity requirements used by other states, the US Government, and other countries around the world.

Recommendation: California should not create its own cybersecurity certification or audit standards. Rather, the CPPA should recognize compliance with existing standards and best practices for cybersecurity risk management as meeting any new California requirements.

Question 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?*

There are significant benefits for both businesses and consumers if the CPPA accepts cybersecurity audits that businesses conduct to comply with leading cybersecurity laws. As explained above, California should not create its own cybersecurity certification or audit standards. Rather, the CPPA should recognize compliance with existing standards and best practices for cybersecurity risk management as meeting any new California requirements.

[8] *See* ISO 27001, ISO - ISO/IEC 27001 — Information security management,NIST Cybersecurity Framework, *available at* https://www.nist.gov/cyberframework/framework.

We recommend the CPPA allow companies to demonstrate compliance with existing cybersecurity laws and standards in two ways:

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

- **Second, the CPPA should allow companies to demonstrate that they have satisfied California's cybersecurity audit requirement through artifacts, such as certifications, attestations, and audit assessment reports, that demonstrate use of practices consistent with existing leading security standards and frameworks.** Given the limited pool of existing auditors with sufficient security expertise, as well as the process involved in conducting a thorough audit, establishing new audit regimes is time-consuming and costly, especially for small businesses and technology consumers that may ultimately absorb such costs. We therefore encourage the CPPA to leverage existing leading security standards and frameworks whenever possible, which will ensure companies are compliant with high standards of data security while reducing both the time delays and costs of demonstrating such compliance.

For example, many organizations may already implement strong data protection safeguards using leading security standards and best practices, including the NIST Cybersecurity Framework, ISO 27001, and Service Organization Controls (SOC) 2 Type 2 certifications. The CPPA's regulations should leverage certifications, attestations, and reports that demonstrate compliance with those existing standards and frameworks. For instance, organizations may engage independent third-party assessment programs to obtain an ISO 27001 certification, which demonstrates conformance with ISO 27001 practices, or may obtain a SOC 2 Type 2 certification after an audit of certain controls like those focused on security or confidentiality, or may obtain FedRAMP authorization, which demonstrates conformance with practices consistent with the NIST Cybersecurity Framework (since both the NIST Cybersecurity Framework and FedRAMP baseline map to NIST 800-53, the U.S. Federal baseline for information security). Compliance with these standards and frameworks should satisfy California's cybersecurity audit requirement. The CPPA should therefore recognize that businesses satisfy California's audit obligations by producing artifacts, such as certifications, attestations, and audit assessment reports, that demonstrate the use of practices consistent with leading standards and frameworks.

One of the standards that California should recognize as satisfying any new cybersecurity requirements is an organization's authorization by the FedRAMP program and the StateRAMP program. FedRAMP is the US Government's approach to the adoption and use of cloud services. FedRAMP aims to grow the use of cloud services (which itself creates opportunities to improve cybersecurity) while reducing duplicative efforts to assess an

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

organization's cybersecurity practices. An organization that earns a FedRAMP authorization or meets similar requirements typically completes a readiness assessment and pre-authorization prior to undergoing a full security assessment and authorization process, and finally engages in continuous monitoring. At the state level, California participates in StateRAMP, which is a multi-state organization that provides state and local governments a common method for verifying an organization's cloud security. Achieving FedRAMP or StateRAMP authorization should be more than sufficient to demonstrate that organizations have adopted cybersecurity practices designed to manage cybersecurity risks, in line with any new CPPA requirements.

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

Recommendation: The CPPA should recognize that compliance with existing best practices for cybersecurity risk management, including existing audits, attestations, and certifications, meet any new California requirements.

Question 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?*

To improve a business's cybersecurity protections, audits and assessments must be robust, and we encourage the CPPA to focus on prioritizing the thoroughness of an audit, which is often distinct from the question of whether an audit is independent. For example, under existing laws a range of different actors may undertake audits or assessments, including both external auditors and audits conducted by internal compliance teams whose role is to assess the company's processes and implement changes across the organization.

The appropriate entity to conduct an audit will vary in different scenarios. For example, businesses may engage third-party auditors to conduct an assessment in a situation where the third party has clear standards to audit against and the business may select an auditor that is certified with a specific accrediting body. SOC audits, for example, are conducted by CPAs and governed by the American Institute of Certified Public Accountants. In contrast, internal audits create an opportunity for continuous monitoring, which can help businesses to identify issues before they become legal, policy, or other business-oriented challenges. Internal audits are also more cost-effective and consequently do not create such high barriers to entry that would have particularly challenging impacts for small businesses.

Recommendation: The CPPA should prioritize robust audits and assessments and recognize that the question of whether an audit is robust is separate from the question of whether it is independent.

Question 5: *What else should the Agency consider to define the scope of cybersecurity audits?*

New regulations are to require businesses whose processing presents a "significant risk" to consumers' security to perform annual cybersecurity audits.

Defining the "significant risk" that triggers this obligation is a key aspect of scoping this obligation. We encourage the CPPA to define processing that presents a "significant risk" to consumers' security in line with, or by reference to, leading cybersecurity laws, policies, and standards. These sources may help the CPPA to flesh out the CCPA's requirement that the definition of "significant risk" consider the "size and complexity of the business and the nature and scope of processing activities."[9] These may include:

- **National Institute of Standards and Technology, Glossary – Definition of High Impact.** NIST has published a glossary of terms that defines "high impact" as a "loss of confidentiality, integrity, or availability [that] could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." Such a loss "might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries." This definition builds on guidance in NIST-FIPS 199, which is used in categorizing federal information and information systems.[10]

- **Securities and Exchange Commission, Guidance on Risk Factors for Identifying Cybersecurity Risks.** The SEC has published guidance intended to help companies identify which cybersecurity risks should be disclosed. It contains a non-exhaustive list that can help companies to identify the risks that are significant enough to make investments speculative or risky. The eight criteria identified by the SEC include the probability of the occurrence and potential magnitude of cybersecurity incidents, the adequacy of preventative actions taken by the company to reduce cybersecurity risks, and the potential costs and consequences of such risks, including industry-specific risks and third-party supplier and service provider risks.[11]

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

II. Privacy Risk Assessments

Under the CCPA, new regulations are to require businesses whose processing of consumers' personal information presents a "significant risk" to consumers' privacy submit to the CPPA "on a regular basis" a risk assessment. The statute identifies information to be included in that assessment and specifies that it does not require businesses to divulge trade secrets.[12]

Privacy risk assessments are an important component of data protection programs. BSA supports requiring businesses to conduct risk assessments for activities that are likely to result in significant privacy risks to consumers. We have therefore supported a range of

[9] Cal. Civil Code 1798.185(15)(A).
[10] NIST – FIPS Pub. 199, Standards for Security Categorization of Federal Information and Information Systems, *available at* https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.
[11] Securities and Exchange Commission, 17 CFR Parts 229 and 249 (Feb. 26, 2018), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.
[12] Cal. Civil Code 1798.185(15)(B).

state privacy laws that require businesses to conduct data protection assessments of high-risk processing activities, which help companies identify and assess potential privacy risks that may arise from those activities and to adopt appropriate mitigation measures. As explained below, a range of countries and states *already* require businesses to conduct data privacy assessments under existing laws. We strongly encourage the CPPA to align California's requirements for privacy assessments with the requirements established by leading global and state laws. This approach will help businesses to invest in a strong set of compliance practices that satisfy multiple legal obligations while identifying and mitigating issues across the business's products and services.

***Question 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?*
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?*

Privacy and data protection laws worldwide require companies that engage in certain activities to conduct privacy risk assessments. These include:

- **European Union General Data Protection Regulation (GDPR).** The GDPR requires controllers to carry out a data protection impact assessment when processing is "likely to result in a high risk to the rights and freedoms of natural persons."[13]

- **UK General Data Protection Regulation (UK GDPR).** Like the GDPR, the UK GDPR requires controllers to carry out data protection impact assessments for processing that is likely to result in a high risk to individuals. The UK's Information Commissioner's Office has published extensive guidance for companies conducting a data protection impact assessment, including a sample template.[14]

- **Colorado Privacy Act**. Colorado's state privacy law will require controllers to conduct a data protection assessment for processing that presents a "heightened risk of harm to a consumer." It defines that term to include: (1) targeted advertising, (2)

[13] GDPR Article 35.
[14] *See* Information Commissioner's Office, Data Protection Impact Assessments, *available at* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments.

profiling that presents certain reasonably foreseeable risks; (3) selling personal data, and (4) processing sensitive data.[15]

- **Connecticut Data Privacy Act**. Connecticut will require controllers to conduct data protection assessments for activities that present a "heightened risk of harm to a consumer." It defines that term to include: (1) targeted advertising, (2) sale of personal data, (3) profiling that presents certain reasonably foreseeable risks, and (4) processing of sensitive data.[16]

- **Virginia Consumer Data Protection Act.** Virginia's law requires controllers to conduct data protection assessments for five types of processing: (1) targeted advertising; (2) sale of personal data, (3) profiling that presents certain "reasonably foreseeable risks"; (4) processing of sensitive data, and (5) any processing activities involving personal data that present a heightened risk of harm to consumers.[17]

In many other countries, regulators are either authorized to require companies to conduct privacy risk assessments in certain contexts or have issued guidance encouraging companies to use privacy risk assessments to satisfy other legal obligations. For example:

- **Brazil General Data Protection Law (LGPD).** Controllers may be required to prepare data protection impact assessments, subject to requirements set out in future regulations by the country's National Agency of Data Protection (ANPD).

- **Singapore Personal Data Protection Act (PDPA)**. Singapore's PDPA does not expressly provide for organizations to conduct data protection impact assessments, but the Personal Data Protection Commission has issued detailed guidance explaining how organizations can use data protection impact assessments to ensure their handling of personal data aligns with the law.[18]

- **Australia Privacy Act**. The Office of the Australian Information Commissioner (OAIC) has published a Privacy Impact Assessment Guide intended to help entities subject to the Australia Privacy Act conduct privacy impact assessments.[19] While the statute does not currently require private-sector companies to conduct such assessments, OAIC has recommended entities use privacy impact assessments to satisfy other legal obligations imposed by the Act, including the requirement to take reasonable steps to implement practices, procedures, and systems that will ensure compliance with the Australia Privacy Principles.[20]

---

[15] Colorado Privacy Act Sec. 6-1-1309(1)-(2).
[16] Connecticut Data Privacy Act Sec. 8(a).
[17] Virginia Consumer Data Protection Act, Sec. 59.1-580.A.
[18] *See* Personal Data Protection Commission of Singapore, Guide to Data Protection Impact Assessments, *available at* https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.pdf; Personal Data Protection Commission of Singapore, Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Revised May 2022), *available at* https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-17-May-2022.pdf.
[19] Office of the Australian Information Commissioner, Guide to Undertaking Privacy Impact Assessments (Sept. 2, 2021), *available at* https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments.
[20] Under the Australia Privacy Act, only government agencies are required to conduct privacy impact assessments. However, the Australian government is undertaking a comprehensive review of the Privacy Act and the Attorney General has recommended that private-sector organizations be required to

The goals and processes of the data protection assessments requirements listed above largely align with the processes and goals articulated in Cal. Civil Code 1798.185(a)(15)(B). Indeed, under many global and state laws, the content of a data protection impact assessment is very similar to the GDPR's requirements. Under Article 35 of the GDPR, a data protection impact assessment must address four topics:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Companies have designed strong global compliance programs that satisfy obligations to conduct data protection impact assessments across multiple jurisdictions. By focusing their investment and resources in compliance practices that satisfy the obligations in more than one country, a business can develop an interoperable global data protection assessment that is better positioned to identify and address issues across the company's products and services. For example, if a company that serves customers in six countries were required to conduct an entirely separate data privacy assessment for each jurisdiction, it may be forced to repeat the same assessment six separate times (or more) — without a clear benefit to consumer privacy. Rather than forcing companies to expend resources to perform the same assessment multiple times, data protection laws can encourage companies to invest in a strong data privacy assessment practice that can be leveraged across jurisdictions. Conducting an interoperable global assessment ensures that a company has time to address and mitigate issues identified in the assessment, rather than simply re-starting the assessment process.

Recommendation: We strongly recommend that the CPPA allow companies to satisfy their obligation to conduct a risk assessment under California law by using risk assessments conducted for the purpose of complying with another jurisdiction's law or regulations. Specifically, we recommend any regulations clearly state that an assessment shall satisfy California's requirements if it is reasonably similar in scope and effect to the data protection assessment that would otherwise be done pursuant to CCPA.

***Question 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 Assessments?

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

conduct privacy impact assessments prior to undertaking a high privacy risk activity. *See* Attorney-General's Department, Privacy Act Review, Report 2022, Recommendation 13.1, *available at* https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.

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?*

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

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

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

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

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

  For other activities, companies are to determine if processing is high risk based on guidance endorsed by the European Data Protection Board (EDPB).[21] That guidance identifies nine criteria to consider in determining if processing is likely to result in high risks to the rights and freedoms of a natural person and suggests an assessment is required if two criteria are met. The criteria are:

  (1) the use of evaluation or scoring;
  (2) automated decision-making with legal or similar significant effects;
  (3) systemic monitoring;
  (4) sensitive data or data of a highly personal nature;
  (5) data processing on a large scale;
  (6) matching or combining datasets;
  (7) data concerning vulnerable data subjects;
  (8) innovative use or applying new technological or organizational solutions; or
  (9) when the processing itself prevents data subjects from exercising a right or using a service or contract.

[21] *See* Article 29 Working Party, Guidelines on Data Protection Impact Assessments, endorsed by EDPB on May 25, 2018, *available at* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

To build on these criteria, data protection authorities (DPAs) in EU member states have created whitelists and blacklists of more specific processing activities intended to complement the guidelines.[22]

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

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

  The Colorado Privacy Act and Connecticut Data Privacy Act require companies to conduct risk assessments of processing that presents a "heightened risk of harm to a consumer."[23] Those laws define such risks to include:

  1. Targeted advertising;
  2. Sale of personal data;
  3. Profiling that presents certain "reasonably foreseeable" risks; and
  4. Processing sensitive data.

  The Virginia Consumer Data Protection Act similarly requires companies to conduct data protection assessments in four specific scenarios. It also includes a broader catch-all provision.[24] Under the Virginia law, assessments are required for the following activities:

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

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

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

---

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

[23] Colorado Privacy Act Sec. 6-1-1309(1)-(2); Connecticut Data Privacy Act Sec. 8(a).

[24] Virginia Consumer Data Protection Act Sec. 59.1-580.A

Question 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?*

California's requirements for privacy risk assessments should mirror CCPA's statutory language, which states that a risk assessment is to address the 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."[25]

As noted above, this statutory language aligns in large part with the requirements of GDPR and of state privacy laws in Virginia, Colorado, and Connecticut.[26]

GDPR Article 35 states:

> The assessment shall contain at least:
> - a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
> - an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
> - an assessment of the risks to the rights and freedoms of data; and
> - the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.[27]

Colorado's Privacy Act states:

> Data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. The controller shall factor into this assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.[28]

[25] Cal. Civ. Code 1798.185(a)(15)(B).
[26] Virginia Consumer Data Protection Act Sec. 59.1-580.B.
[27] GDPR Article 35.
[28] Colorado Privacy Act Sec. 6-1-1309(3).

Connecticut's Data Privacy Act states:

> Data protection assessments conducted pursuant to subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.[29]

Virginia's CDPA states:

> Data protection assessments conducted pursuant to subsection A shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.[30]

Recommendation: The requirements for privacy risk assessments in California should mirror the CCPA's statutory text. That text aligns in large part with leading global data protection laws and state privacy laws.

Question 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?*

There are significant benefits to both businesses and consumers if the CPPA accepts the submission of risk assessments that were completed in compliance with the GDPR or the Colorado Privacy Act, or other laws with requirements reasonably similar in scope or effect.

In many cases, companies that do business across state and national boundaries have already established processes for conducting and documenting privacy-related risk assessments, including under global privacy laws like the EU's GDPR, Brazil's LGPD, and the obligations imposed by state laws in Colorado, Connecticut, and Virginia. Companies are better positioned to detect and respond to privacy concerns identified through a privacy risk assessment if they invest in a strong and centralized privacy assessment process that can be leveraged for compliance with the range of privacy and data protection laws to which the company's processing activities are subject.

In contrast, if the CPPA adopts regulations that require separate (and overlapping) assessments, it will fragment compliance efforts—a diversion of resources that should

[29] Connecticut Data Privacy Act Sec. 8(b).
[30] Virginia Consumer Data Protection Act Sec. 59.1-580.B.

reflect an intentional choice rather than an unintentional consequence of creating regulations that do not account for existing laws, frameworks, and compliance mechanisms.

Recommendation: We strongly recommend that the CPPA allow businesses to satisfy their obligation to conduct a privacy risk assessment under California law by using risk assessments conducted for the purpose of complying with another jurisdiction's law or regulations. Specifically, we recommend any regulations clearly state that an assessment shall satisfy California's requirements if it is reasonably similar in scope and effect to the data protection assessment that would otherwise be done pursuant to CCPA.

Question 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)?*

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

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

In addition, the regulations should provide that the CPPA will treat risk assessments provided to the agency as confidential and not subject to public disclosure and make clear that the disclosure of those assessments to the agency does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections.[31] This will not only help avoid inadvertent disclosure of proprietary data and business practices that may be reflected in a risk assessment, but will also help ensure strong incentives for companies to undertake rigorous risk assessments.

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

[31] Other states provide such protection. *See, e.g.*, Colorado Privacy Act Sec. 6-1-1309(4); Connecticut Data Privacy Act Sec. 8(c); Virginia Consumer Data Protection Act Sec. 59.1-576.C.

III. Automated Decision-Making

Under the CCPA, new regulations are to govern "access and opt-out rights with respect to business' use of automated decision-making technology, including profiling." Regulations are also to require that business' response to access requests include "meaningful information about the logic involved" in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.[32]

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

Access Rights. In the United States, all five states to enact comprehensive privacy laws create rights for consumers to access personal information. These access rights are not limited to personal information processed in connection with automated decision-making, but apply to a much broader range of processing activities. Like other state privacy laws, the CCPA creates a right for consumers to request certain information from a business that collects personal information about the consumer.

Because the CCPA already gives consumers a broad right of access, the CPPA should not create a separate — and potentially duplicative — access right focused only on access in connection with automated decision-making. Instead, the CPPA should focus any new regulations on addressing how the statute's existing access right applies in the context of automated decision-making.

Opt-Out Rights. In the United States, comprehensive state privacy laws in three states create clear statutory rights for individuals to opt out of certain automated decision-making activities that amount to "profiling." Those states are Colorado, Connecticut, and Virginia.

Colorado's Privacy Act states:

> A consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of . . . profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.[33]
>
> Profiling is defined 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."[34]

[32] *See* Cal. Civil Code Sec. 1798.185(16).
[33] *See* Colorado Privacy Act Sec. 6-1-1306(1)(a)(I)(C). "Decisions that product legal or similarly significant effects concerning a consumer" are defined as "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." *Id.* at Sec. 6-1-1303(10).
[34] *Id.* at Sec. 6-1-1303(20).

Connecticut's Data Privacy Act states:

> A consumer shall have the right to: . . . opt out of the processing of the personal data for purposes of . . . profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer[35].
>
> Profiling is defined as "any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[36]

Virginia's Consumer Data Protection Act states:

> A controller shall comply with an authenticated consumer request to exercise the right . . . [t]o opt out of the processing of the personal data for purposes of . . . .(i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.[37]
>
> Profiling is defined as "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[38]

Unlike the statutory language in Colorado, Connecticut, and Virginia, the CCPA's text does not clearly call for a stand-alone right to opt out of certain types of automated decision-making. Rather, the statutory text narrowly focuses on the use of automated decision-making in the context of the access and opt-out rights already included in CCPA. The plain language of the statue accordingly calls for regulations that identify how the existing access and opt-out rights operate in the context of businesses using automated decision-making technology, including profiling. This reading of the statute is confirmed by the next part of the CCPA's text, which focuses on how the access right works in this context, by requiring businesses to provide "meaningful information about the logic involved" in such automated decision-making processes and a description of the likely outcome of such processes.

Conversely, adopting a broader reading of the CCPA's language would seem to exceed the statutory text, which does not envision regulations that contain the type of automated decision-making rights found in GDPR or the rights to opt out of certain types of profiling found in the Colorado, Connecticut, and Virginia state privacy laws.[39] While we appreciate the

---

[35] Connecticut Data Privacy Act Sec. 4(a)(5)(C).
[36] *Id.* Sec. 1(22). "Decisions that produce legal or similarly significant effects concerning the consumer" are defined as "decisions made by the controller that result in the provision or denial by the controller 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." *Id.* at Sec. 1(12).
[37] Virginia Consumer Data Protection Act Sec. 59.1-577.A.5(iii).
[38] *Id.* at Sec. 59.1-575. "Decisions that produce legal or similarly significant effects concerning a consumer" are further defined as "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water."
[39] *See, e.g.*, GDPR Article 22 (stating that data subjects have a right "not to be subject to a decision based solely on automated processing . . . which produces legal effects concerning him or her or

role that a strong data privacy law can play in ensuring that automated decision-making technology is used in responsible ways, and we believe focusing on these issues is needed as the underlying technology continues to be developed, the upcoming regulations do not appear to be the forum best suited to addressing these issues, given their narrow scope.

Recommendation: New regulations should focus on how existing access and opt-out rights created by the CCPA apply in the context of automated decision-making technology, in line with the statute's narrow text.

Question 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 decision-making technology" defined? Should the Agency adopt any of these definitions? Why, or why not? 7 Civ. 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 decision-making technology requirements?*
d. *What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decision-making? 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 decision-making? 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?*

If the CPPA creates a new right to opt out of profiling, we strongly recommend that right be defined in line with the rights already established in Colorado, Connecticut, and Virginia's privacy laws. These laws share important similarities, including:

- *Creating a right to opt-out of profiling for decisions with "legal or similarly significant effects."* Focusing a right to opt out of profiling on a core set of decisions about individuals is critical to ensure any right is not so broad or vague that it would be impractical to implement in practice. As noted earlier, the three existing state laws that create rights to opt out of profiling activities apply to decisions with "legal or similarly significant effects" and define that term in similar ways. For example, Connecticut's law defines such effects to mean "decisions made by the controller that result in the provision or denial by the controller 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."[40] Virginia and Colorado define the term similarly.[41]

similarly significantly affects him or her"); Virginia Consumer Data Protection Act Sec. 59.1-573 (creating a right to opt out of profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer"); Colorado Privacy Act Sec. 6-1-1306(a)(I)(C) (granting same right to opt out of profiling as Virginia law).

[40] Connecticut Data Privacy Act Sec. 1(12).

[41] Virginia Consumer Data Protection Act Sec. 59.1-575; Colorado Privacy Act Sec. 6-1-1303(10).

- *Creating a right that applies to final decisions*. As Colorado, Connecticut, and Virginia's state privacy laws recognize, a right to opt out of certain profiling activities should apply to final decisions made by a company. For example, Connecticut's right to opt out of profiling applies to certain "*decisions made by the controller* that *result in the provision or denial* by the controller," of certain services or opportunities.[42] Virginia and Colorado's laws similarly focus on final decisions.

Because the Colorado, Connecticut, and Virginia privacy laws all create a clear statutory right to opt out of profiling, companies have already designed and implemented processes for responding to requests to opt out of profiling covered by those laws.

As noted above, the CCPA's plain text does not appear to contemplate the creation of a stand-alone right to opt out of profiling. However, if the CPPA does create a right to opt out of profiling under California law, aligning that right with the existing rights created by other state laws would allow California consumers to use the processes that businesses have already established to comply with this new right. To the extent California creates a right to opt out of profiling that does not align with those created in other states, companies may be required to create a separate process for complying with California requests. In practice, the more separate processes a company must establish to comply with similar types of consumer requests, the more difficult it becomes to maintain and improve those processes. Different but overlapping processes that vary among states are also likely to increase confusion for consumers. Companies that can establish a single process to comply with rights to opt out of profiling are better positioned to update that process across products and services based on practical experience and consumer feedback, leading to better outcomes for consumers.

Recommendation: If the CPPA creates a new right to opt out of profiling under California law, it is important to align that right with existing rights created by other state laws so that California consumers can use established and centralized processes to exercise their right. Any right should: (1) apply to decisions that produce "legal or similarly significant effects," and (2) apply only to final decisions, in line with other state privacy laws.

Question 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 decision-making 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?

The CPPA contemplates that new regulations will require businesses responding to access requests to provide "meaningful information about the logic involved" in automated decision-making processes, as well as "a description of the likely outcome of the process with respect to the consumer."[43] This language mirrors the GDPR, which creates a right for individuals to access certain information when their personal data is processed for profiling, including "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[44]

[42] Connecticut Data Privacy Act Sec. 1(12) (emphasis added).
[43] *Id.*
[44] *See* GDPR Article 15(1)(h).

European regulators applying this standard have emphasized the need for "simple" explanations that do not confuse consumers. We encourage the CPPA to apply the CCPA's requirement in a similar manner, by focusing on providing simple and understandable information to consumers. In addition, we encourage the CPPA to ensure any new regulations on access requests do not jeopardize trade secret protections.

European Data Protection Board (EDPB). Guidance endorsed by the EDPB addresses how controllers can provide meaningful information about automated decision-making processes, emphasizing the need for individuals to understand the information provided.[45] That guidance states:

> The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.

UK Information Commissioner. Similarly, the UK ICO has focused on applying this standard to require controllers to provide information that does not confuse a consumer.[46] The ICO's guidance states:

> Providing 'meaningful information about the logic' and 'the significance and envisaged consequences' of a process doesn't mean you have to confuse people with over-complex explanations of algorithms. You should focus on describing:
> - the type of information you collect or use in creating the profile or making the automated decision;
> - why this information is relevant; and
> - what the likely impact is going to be/how it's likely to affect them.

Recommendation: The CCPA's requirement to provide "meaningful information" about automated decision-making systems should be applied in a practical manner, to focus on providing simple and understandable information to consumers. In addition, any new regulations on access requests should not jeopardize trade secret protections.

Question 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?*

As with other rights created in the CCPA, it is important that any new regulations continue to recognize that consumers are to exercise access and opt-out rights by going directly to a business, rather than to its service providers.

---

[45] *See* Article 29 Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Oct. 3, 2017, revised Feb. 6, 2018), endorsed by European Data Protection Board (EPDB) on May 25, 2018, *available at* https://ec.europa.eu/newsroom/article29/items/612053/en.

[46] UK Information Commissioner Office, What Else Do We Need to Consider if Article 22 Applies, *available at* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/.

Although the CCPA primarily focuses on businesses, which "determine[] the purposes and means of the processing of consumers' personal information,"[47] the statute also recognizes that businesses may engage service providers to "process[] personal information on behalf of a business."[48] Service providers must enter into written contracts with businesses they serve, limiting how the service provider can retain, use, and disclose personal information provided to them by a business. In this way, the CCPA ensures that personal information is subject to statutory protections both when a business collects and processes a consumer's personal information itself, and when that business hires service providers to process a consumer's personal information on its behalf. The statute also recognizes the distinct roles of businesses and service providers by assigning them different obligations based on their different roles in handling consumers' personal information.

Under the CCPA, businesses are assigned the responsibility of responding to consumers' requests to access, correct, and delete their personal information. This is consistent with all other state consumer privacy laws and leading data protection laws worldwide, which place this obligation on companies that decide how and why to collect consumers' data — rather than the service providers acting on behalf of such companies. If the CPPA creates a new right to opt out of profiling via regulations, that right should similarly be exercised by the consumer going directly to the business.

Recommendation: As the CCPA contemplates new regulations addressing access and opt-out rights, it should ensure those rights continue to reflect the statute's recognition of the distinct roles of businesses and service providers.

* * *

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

—

For further information, please contact:
Kate Goodloe, Managing Director, Policy
kateg@bsa.org

[47] Cal. Civ. Code 1798.140(d)(1).
[48] Cal. Civ. Code 1798.140(ag)(1).