BSA | The Software Alliance

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

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

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

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

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

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

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

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

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

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

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

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

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

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

I. Cybersecurity Audits

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

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

A. Defining Significant Risk to Security

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

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

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

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

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

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

B. Leveraging Existing Standards and Best Practices

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

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

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

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

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

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

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

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

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

II. Risk Assessment Requirements

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

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

A. Defining Significant Risk to Privacy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Providing Risk Assessments to the CPPA

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

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

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

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

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

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

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

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

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

A. The Distinct Role of Service Providers

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

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

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

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

B. Service Providers Need to Combine Personal Information

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

These include:

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

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

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

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

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

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

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

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

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

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

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

IV. Automated Decision-Making

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

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

---

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

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

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

V. Agency Audits

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

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

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

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

---

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

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

VI. Harmonizing the Regulations

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

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

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

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

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

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

* * *

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

___

For further information, please contact:

Kate Goodloe, Senior Director, Policy
kateg@bsa.org or 202-530-5122

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