BSA | The Software Alliance

Submission to the California Privacy Protection Agency on Modified Proposed Regulations Implementing the Consumer Privacy Rights Act of 2020

BSA | The Software Alliance appreciates the opportunity to submit comments regarding the modified text of the proposed regulations ("Modified Proposed Regulations") implementing the California Privacy Rights Act of 2020 ("CPRA"), which amended the California Consumer Privacy Act ("CCPA"). We appreciate the California Privacy Protection Agency's ("CPPA's") work to address consumer privacy and to develop regulations that protect the privacy of Californians' personal information.

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 three aspects of the Modified Proposed Regulations:

1. ***Role of Service Providers.*** The CCPA recognizes that businesses and service providers play different roles in protecting consumer privacy — and are therefore assigned different obligations under the statute based on their different relationships with consumers. We appreciate a range of changes made in the Modified Proposed Regulations to better reflect these distinct roles. However, we strongly suggest revising three aspects of the Modified Proposed Regulations to carry those changes throughout the regulations. First, the Modified Proposed Regulations should be revised to further clarify a service provider's role in responding to consumer rights requests — including by continuing to recognize that service providers may fulfill their

[1] BSA's members include: BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, 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

role of assisting businesses by creating tools that enable a business to respond to consumer rights requests for data held by the service provider. Second, the Modified Proposed Regulations should avoid creating data minimization obligations that depend on a consumer expectations about the role of service providers or how "apparent" a service provider's activity is to consumers. Third, the contractual requirements for service providers in the Modified Proposed Regulations should be revised to align with the CCPA's statutory text.

2. ***Global Opt-Out Mechanism.*** The CPPA is tasked with issuing regulations to implement a global opt-out mechanism. Although we believe the CCPA is best read to permit (but not require) companies to honor requests submitted through global opt-out mechanisms, it is critical that any opt-out mechanism recognized by the Modified Proposed Regulations (whether mandatory or voluntary) be interoperable with mechanisms recognized by other states and function in practice. Accordingly, the Modified Proposed Regulations should account for potentially conflicting opt-out requirements and the CPPA should work with other state regulators to ensure that opt-out requirements are consistent across state lines. We also strongly recommend the CPPA prioritize addressing practical issues around implementing opt-out mechanisms, including how businesses are to determine a mechanism meets the CCPA's requirements. For example, one way to address such concerns is for the CPPA to publish a list of the signals that meet CCPA's requirements and thus identify the mechanisms that businesses should honor.

3. ***Agency Audits.*** The Modified Proposed Regulations provide few details on the agency's audit authority — and create few guardrails to ensure the agency exercises its audit authority in a manner that does not inadvertently create privacy and security risks. We recommend revising the Modified Proposed Regulations to create such guardrails, including limiting the use of on-site audits, which can present significant privacy and security risks not accounted for in the Modified Proposed Regulations.

I. Role of Service Providers

Although the CCPA primarily focuses on businesses, which "determine[] the purposes and means of the processing of consumers' personal information,"[2] the statute also recognizes that businesses may engage service providers to "process[] personal information on behalf of a business."[3] 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.

We urge three types of revisions to the Modified Proposed Regulations to better reflect the role of service providers, consistent with the CCPA's statutory text.

A. The Modified Proposed Regulations Should Be Revised to Better Reflect the Role of Service Providers in Responding to Consumer Rights Requests

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

[2] Cal. Civ. Code § 1798.140(d)(1).
[3] Cal. Civ. Code § 1798.140(ag)(1).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

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.

Of course, consumer rights must work in practice — even when personal information is held by a service provider. That is why the CCPA requires service providers to assist a business in fulfilling rights requests for personal information. Under the CCPA, service providers may either execute consumer rights requests directly or ***enable a business*** to do so. This second option — enabling the business to respond to requests — is critical to ensuring that companies can respond to large volumes of consumer rights requests efficiently and effectively. For example, many service providers offer services at scale that are used by hundreds of business customers, each of which may receive thousands of consumer rights requests. Service providers can help their business customers efficiently respond to those requests by creating scalable tools that the business can use to access, correct, and delete information held by the service provider — and thereby establish processes for assessing and responding to a large volume of requests.

We appreciate several changes made by the Modified Proposed Regulations to address this issue, including in Section 7022. We strongly agree with retaining the proposed text throughout Section 7022(b) that clarifies a business is either to notify a service provider to delete a consumer's personal information or, if enabled to do so by the service provider, delete the personal information itself. We encourage two further revisions to carry these changes throughout the Modified Proposed Regulations.

Recommendation: The Modified Proposed Regulations should be further revised to align with the CCPA's clear recognition that service providers may fulfil their role in handling consumer rights requests by either executing those requests or by ***enabling the business*** to do so. We strongly recommend two sets of changes:

1. Section 7022(f)(4), which addresses instances in which a business denies a consumer's request to delete in whole or part, should either be deleted or should be revised in line with changes made throughout this section that recognize a service provider may enable the business to comply with requests for data held by the service provider. If this provision is retained, we strongly recommend revising it to state a business is required to: "Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception, or if enabled to by the service provider, the business shall comply with the portion of the request not subject to the exception."

2. Three of the modified provisions in Section 7022 should be further revised to focus on personal information a service provider "processes" pursuant to a contract, rather than information it "collects." This change better aligns with the CPRA's statutory language, which defines a service provider as "a person that ***processes*** personal information on behalf of a business" rather than one that *collects* personal information on behalf of a business.[4] Moreover, the CPRA defines processing broadly, to include "any operation" performed on personal information. Aligning the regulations with this statutory definition ensures their scope mirrors the scope of a service provider's role under the statute. We suggest:

[4] Cal. Civ. Code § 1798.140(ag)(1) (emphasis added).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

i. Revising Section 7022(b)(2) to state: "Notifying the business's service providers or contractors to delete from their records the consumer's personal information that they Processed ~~Collected~~ pursuant to their written contract with the business, or if enabled to do so by the service provider or contractor, the business shall delete the personal information that the service provider or contractor Processed ~~Collected~~ pursuant to their written contract with the business; and"

ii. Revising Section 7022(c) to state: "A service provider or contractor shall, with respect to personal information that they Processed ~~Collected~~ pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by:

iii. Revising Section 7022(c)(3) to state: "Notifying any of its own service providers or contractors to delete from their records in the same manner the consumer's personal information that they Processed ~~Collected~~ pursuant to their written contract with the service provider or contractor."

B. The Modified Proposed Regulations Should Not Focus on the Degree to Which The Involvement of Service Providers is "Apparent" to Consumers

The Modified Proposed Regulations include a range of obligations intended to ensure a business's collection, use, retention and/or sharing of personal information is reasonably necessary and proportionate to achieve certain purposes permitted by the statute. Section 7002, for example, focuses on ensuring that the purposes for which personal information are collected or processed are consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. Section 7002(b) sets out several factors that may bear on a consumer's expectations about why her data will be used, including the relationship between the consumer and the business and the type, nature, and amount of personal information that the business seeks to collect or process.

Section 7002(b)(5)'s treatment of service providers creates significant concerns. Although several other factors addressed in Section 7002(b) may appropriately bear on consumer expectations, Section 7002(b)(5) treats the "degree to which the involvement of service providers" is "apparent" to consumers as a factor in determining consumer expectations.

This provision is fundamentally at odds with the role of service providers, which process personal information on behalf of businesses. Consumers generally expect to interact with consumer-facing businesses, and not the dozens or more service providers who may process personal information on behalf of a single business. Of course, personal information should be safeguarded when processed by service providers, which is why CCPA and other leading privacy and data protection laws apply a range of other requirements to service providers to ensure they only process data on behalf of and at the direction of businesses. But those safeguards do not — and should not — turn on whether consumers expect a business to use a service provider, or whether the service provider's role is "apparent" to a consumer.

Service providers are most valuable to both consumers and businesses when they help companies deliver products seamlessly. In many cases, a business will rely on a range of service providers to deliver a single product, with each service provider acting on behalf of and at the direction of that business. For example, a grocery store that accepts online and mobile orders may have many service providers: one service provider to store consumers' orders and other information in the cloud; a second service provider to text consumers when their orders are out for delivery; and a third service provider to maintains the store's mobile application. Even though these activities rely on service providers, the text messages and

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

mobile app bear the grocery store's name — because the service providers are merely processing personal information on its behalf and at its direction. If businesses were required to make the use of service providers "apparent" to consumers, the ability to offer these seamless services in the name of the consumer-facing business that an individual expects to interact with would decrease significantly. We strongly recommend deleting Section 7002(b)(5), to avoid this result.

Recommendation: Section 7002(b)(5) should be deleted in its entirety. Alternatively, we recommend revising this provision to delete references to service providers, which are subject to additional safeguards in handling personal information under CCPA not applicable to other entities such as third parties.

1. If Section 7002(b)(5) is not deleted, it should be revised to state: "The degree to which the involvement of ~~service providers,~~ contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). For example, the consumer likely expects an online retailer's disclosure of the consumer's name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider's involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a third party ~~service provider~~ if the consumer is not directly interacting with the third party ~~service provider~~ or the third party's ~~service provider's~~ role in the processing is not apparent to the consumer.

C. The Modified Proposed Regulations Should Not Create Contractual Obligations Beyond Those Set out in the CCPA's Text.

Two provisions of the CCPA create statutory requirements for contracts between businesses and service providers. First, Section 1798.100(d) requires businesses that engage service providers to enter into agreements with such providers. Second, in the CCPA's definition of the term "service provider" in Section 1798.140(ag), the statute requires that service providers be subject to contractual limitations in handling data on behalf of businesses.[5] Beyond these requirements, the CCPA allows businesses and service providers to craft their own contracts. This is important, because it allows the parties to evaluate the nature of their relationship, the information to be processed, and the role of the service provider, and tailor the agreement accordingly.

---

[5] Under Section 1798.140(ag), a service provider must process data pursuant to a contract that prohibits it from:

- "[S]elling or sharing the personal information[.]"
- "Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by [the CCPA]."
- "Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business."
- "Combining the personal information that the service provider receives from, or on behalf of, the business with [other] personal information . . . provided that the service provider may combine personal information to perform any business purpose as defined in regulations [to the CCPA]" other than in connection with cross-context behavioral advertising, or marking and advertising for consumers who exercised their opt-out rights.

This provision goes on to note that "the contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months."

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

However, the Modified Proposed Regulations create contractual requirements that go beyond those in the statute. We recommend revising the Modified Proposed Regulations to better align with the CCPA's requirements.

1. Section 7051(a)(7) of the Modified Proposed Regulations appears to conflate two separate provisions of the CCPA.

Section 7051(a)(7) of the Modified Proposed Regulations states that contracts between a business and a service provider must:

> Grant the business the right to take reasonable and appropriate steps to ensure that service provider uses the personal information that it Collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.[6]

This provision combines two separate statutory requirements, in a manner that can be read to impose additional contractual obligations beyond those in the statute. The first part of this provision is based on CCPA Section 1798.100(d)(3), which states that a contract between a service provider and a business must "[g]rant[] the business rights to take reasonable and appropriate steps to help ensure that the . . . service provider . . . uses the personal information transferred in a manner consistent with the business' obligations under this title."[7] The second part is based on the CCPA's definition of service provider in 1798.140(ag)(1)(D), which states that the contract "may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months."[8]

Section 7051(a)(7) of the Modified Proposed Regulations combines these two statutory provisions, in a manner that suggests several contractual commitments may be mandatory — even though the CCPA clearly makes those commitments permissive rather than required. Specifically, Section 7051(a)(7) could be read to suggest that the compliance monitoring steps set out in the CCPA's definition of a service provider (as actions that may be taken "subject to agreement with the service provider") could be viewed as required provisions of a service provider contract. This is not consistent with the text of the statute, which allows parties to agree to the "reasonable and appropriate steps" suitable in the context of a given service. The Modified Proposed Regulations should be revised to avoid suggesting otherwise.

Recommendation: Section 7051(a)(7) of the Modified Proposed Regulations should be revised to delete this ambiguous language, so that the provision states that contracts between businesses and service providers shall: "(7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it Collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. ~~Reasonable and appropriate steps may include ongoing manual reviews and automated~~

[6] Mod. Prop. Reg. § 7051(a)(7).
[7] Cal. Civ. Code § 1798.100(d)(3).
[8] Cal. Civ. Code § 1798.140(ag)(1)(D) (emphasis added).

~~scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.~~"

2. Section 7051(a)(2) of the Modified Proposed Regulations appears to require specificity in contracts that goes beyond the CCPA's requirements.

Section 7051(a)(2) of the Modified Proposed Regulations requires service provider contracts to "[i]dentify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business."[9] It also states: "[t]he Business Purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific."[10]

This requirement to provide "specific" business purposes goes beyond the requirements of the CCPA. The statute affords service providers and businesses greater flexibility to identify the business purposes for which a service provider may process personal information — including by referring to their contract as appropriate. This flexibility is important because it helps to avoid the need for businesses and service providers to continually amend and re-negotiate data processing terms as new services are added to a contract. The requirement to provide each "specific" business purpose is not necessary to ensure that data remains protected when processed by a service provider, because the service provider is already required to handle data in line with the contract with the business and subject to safeguards set out in the statute. Requiring greater specificity about the "specific" purposes for processing covered by a contract is also unlikely to create a substantial benefit to consumers, given the statutory limits already imposed on both businesses and service providers.

Recommendation: Section 7051(a)(2) of the Modified Proposed Regulations should be revised to be consistent with the CCPA, as follows: "Identify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified Business Purpose(s) set forth within the contract. ~~The Business Purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.~~"

3. Sections 7050 and 7051 Should Be Revised to Recognize that Service Providers "Process" Personal Information

Sections 7050 and 7051 address a number of contractual and other obligations placed on service providers under the CCPA. Throughout the recently-revised text, however, the Modified Proposed Regulations refer to personal information that a service provider "collected" pursuant to its written contract with a business. We strongly recommend revising this language to better align with the CCPA's statutory text, which defines a service provider as "a person that ***processes*** personal information on behalf of a business" rather than one that *collects* personal information on behalf of a business.[11]

Recommendation: In addition to other recommended edits addressed above, seven provisions in Sections 7050 and 7051 should be revised to replace "collect" with "process":

---

[9] Mod. Prop. Reg. § 7051(a)(2).
[10] *Id.*
[11] Cal. Civ. Code § 1798.140(ag)(1) (emphasis added).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

1. Section 7050(a) should be revised to state: "A service provider or contractor shall not retain, use, or disclose personal information Processed ~~Collected~~ pursuant to its written contract with the business except:"

2. Section 7051(a)(1) should be revised to state: "Prohibit the service provider or contractor from selling or sharing personal information it Processes ~~Collects~~ pursuant to the written contract with the business."

3. Section 7051(a)(3) should be revised to state: "Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Processes ~~Collected~~ pursuant to the written contract with the business for any purpose other than the Business Purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations."

4. Section 7051(a)(4) should be revised to state: "Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Processes ~~Collected~~ pursuant to the written contract with the business for any commercial purpose other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations."

5. Section 7051(a)(5) should be revised to state: "Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Processes ~~Collected~~ pursuant to the written contract with received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it Processes ~~Collected~~ pursuant to the written contract with received from, or on behalf of, the business with personal information that it received from another source or Processes ~~Collected~~ from its own interaction with the consumer, unless expressly permitted by the CCPA or these regulations."

6. Section 7051(a)(6) should be revised to state: "Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it Processes ~~Collected~~ pursuant to the written contract with the business—providing the same level of privacy protection as required by of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and to implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5."

7. Section 7051(a)(7) should be revised to state: "Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it Processes ~~p~~ pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months."

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

II. Global Opt-Out Mechanism

A. Any Global Opt-Out Mechanism Should be Consistent and Interoperable with Mechanisms Recognized by Other State Privacy Laws.

BSA believes that consumers should have clear and easy-to-use methods for exercising new rights given to them by any privacy law.

Under the CCPA, the CPPA is tasked with issuing regulations that define the requirements and technical specifications for an opt-out preference signal that indicates a consumer's intent to opt out of the sale or sharing of that consumer's personal information, and to limit the use or disclosure of the consumer's sensitive personal information. In our view, the best reading of the CCPA, as amended by CPRA, is that any such opt-out mechanism is permitted, but not required, by the statute.[12] The Modified Proposed Regulations, however, contemplate a mandatory opt-out preference mechanism and require businesses to process opt-out preference signals meeting the requirements in Section 7025.

Regardless of whether a global opt-out mechanism is permissive or required, it is critically important that businesses understand which mechanism(s) they are to honor — and that those mechanisms be interoperable with any similar mechanisms recognized by other states. In particular, the new consumer privacy laws in Colorado and Connecticut create clear statutory requirements for companies to honor global opt-out mechanisms starting July 1, 2024 (for Colorado) and January 1, 2025 (for Connecticut). We strongly recommend the CPPA engage with regulators in those states to ensure that any global opt-out mechanism recognized in California is consistent and interoperable with opt-outs under these other state laws.

Recommendation: The CPPA should work with regulators in other states to ensure any opt-out mechanism recognized in California is interoperable with mechanisms recognized in other states.

B. Any Global Opt-Out Mechanism Must Function in Practice.

It is also critical that both businesses and consumers be able to use global opt-out mechanisms in practice. However, the Modified Proposed Regulations do not address a range of practical issues that will confront businesses and consumers as these mechanisms are implemented.

For example, is not clear from the Modified Proposed Regulations how a business will be able to determine that a particular signal meets the requirements of Section 7025(b), or if that determination will be left to each business. Likewise, consumers will not know which mechanisms will be honored or to what extent a mechanism will be honored across state lines. One way to address such concerns is for the CPPA to publish a list of the signals that meet CCPA's requirements and thus identify the mechanisms that businesses should honor, but the Modified Proposed Regulations do not clearly contemplate such a process. Creating a clear way for businesses to understand which mechanisms they must honor is important to ensuring that these mechanisms function in practice.

The CPPA should address such practical issues, to help ensure that businesses have fair notice of the mechanisms they may use to comply with obligations under the CCPA and can implement them in a manner that is easy for consumers to use. Companies will require time

[12] *See* Cal. Civ. Code 1798.135(b)(3) (stating that a business that complies with provisions for providing consumers certain opt-out links "is not required to comply with subdivision (b) [governing opt-out preference signals]. For the purpose of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b)").

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

to build tools to respond to global opt-out mechanisms — and focusing on practical issues early on will help foster the development and implementation of tools that work in practice.

Recommendation: The CPPA should address practical considerations including how a business will recognize if a particular signal meets the regulations' requirements. For example, the CPPA could develop a process for approving an opt-out signal and then publish a list of compliant signals; it could also work with stakeholders to create a process for nominating additional signals for the agency's approval, to help companies and consumers implement opt-out mechanisms in practice.

C. Consumer Education Around Global Opt Outs and Their Potential Limitations Will be Critical.

The CPPA should also prioritize educating consumers about global opt-out mechanisms and specifically the scope of what such mechanisms do, as well as their limitations. For example, if a consumer uses a browser-based mechanism to opt out of the sale or sharing of the consumer's personal information, the browser may be able to effectuate that request for activity that occurs within the browser, but not activity outside of the browser. Consumers should be aware of this and other limitations. The CPPA, and developers of compliant opt-out signals, are well-positioned to provide that education.

Recommendation: The CPPA should prioritize educating consumers about global opt-out mechanisms, including their scope and their limitations.

III. Agency Audits

A. The CPPA Should Exercise its Audit Authority in a Manner that Minimizes Privacy and Security Risks to Consumers, Including by Limiting On-Site Audits.

Under the CCPA, the CPPA is granted authority to audit compliance with the law and is tasked with issuing regulations to define the scope of the agency's authority and the process for exercising that authority. In particular, the statute requires that these regulations include establishing criteria for both selecting persons to audit and for "protect[ing] consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena."[13]

The Modified Proposed Regulations provide few details about — or guardrails for — this authority. Section 7304 of the Modified Proposed Regulations states that the CPPA "may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA."[14] But the regulations do not address how personal information will be protected from disclosure in the absence of a court order, warrant, or subpoena, as required by the statute. Nor do the Modified Proposed Regulations clearly state how privileged information will be handled. Rather, the Modified Proposed Regulations state only that consumers' personal information disclosed to the agency during an audit will be maintained in compliance with the state's Information Practices Act of 1977.

We strongly recommend that the Modified Proposed Regulations create additional safeguards to ensure that audits further the CCPA's goal of protecting consumer privacy — and also that ensure the audit authority is not exercised in a manner that could inadvertently undermine consumer privacy or cybersecurity.

[13] Cal. Civ. Code § 1798.185(a)(18).
[14] Mod. Prop. Reg. § 7304(a).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

In particular, the Modified Proposed Regulations should be revised to address how audits will be conducted — including whether they will occur on-site or off site — and to specifically limit the use of on-site audits absent specific circumstances warranting an on-site audit. Any audit should require guardrails to mitigate the potentially significant privacy and security concerns involved. For example, an audit of a service provider that serves hundreds of businesses can create a range of privacy and security risks. This is particularly true when the audit is on-site, as opposed to remote. An on-site audit may inadvertently expose to auditors information relating to a range of businesses and consumers whose activities are not the intended focus of the audit, creating significant privacy risks. Moreover, in this context on-site audits would typically not provide information beyond that available through a remote audit, because the relevant information is accessible in either case. Indeed, remote audits can be more efficient in identifying relevant information without the attendant privacy and security risks of an on-site audit.

We recommend revising the Modified Proposed Regulations to limit the use of on-site audits and specifically endorse the use of remote audits, particularly when there are no special circumstances that merit the audit being conducted on-site and when an on-site audit may create privacy and security concerns. Given the privacy and security risks that arise from exercising the agency's audit authority, we urge the CPPA to limit the use of its audit authority to circumstances in which there is a "significant" concern that the statute has been violated. The agency may define such circumstances by example, consistent with other aspects of the Modified Proposed Regulations.

Recommendation: We make two recommendations to focus the Agency's audit authority:

1. Section 7304(a) should be revised to state: "(a) Scope. The Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA. Audits will be conducted remotely, absent specific circumstances warranting an on-site audit. Where specific circumstances warrant more immediate intervention, the Agency shall require in writing the preservation of documents and information."

2. Section 7304(b) should be revised to state: "(b) Criteria for Selection. The Agency may conduct an audit in circumstances that create a significant risk of ~~to investigate~~ possible violations of the CCPA. Alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA ~~or any other privacy protection law~~."

* * *

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