BSA | The Software Alliance

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

BSA | The Software Alliance appreciates the opportunity to submit comments regarding the proposed regulations ("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 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. Although many aspects of the Proposed Regulations reflect these unique roles, we strongly suggest revising two areas that risk upsetting the careful statutory assignment of responsibilities between businesses and service providers. First, the Proposed Regulations should be revised to clarify a service provider's role in responding to consumer rights requests – including recognizing that service providers may fulfill their role of assisting a business by creating a tool that enables the business to respond to consumer rights requests for data held by the service provider. Second, the Proposed Regulations' contractual requirements for service

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, 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

providers should be limited to the requirements set forth in the statute, which ensures businesses and service providers can tailor agreements to the context of their relationship. In addition, we recommend the Proposed Regulations retain helpful examples that make clear that service providers can combine personal information to improve services offered at scale.

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 Proposed Regulations (whether mandatory or voluntary) be interoperable with mechanisms recognized by other states and function in practice. Accordingly, the 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 how any opt-out mechanism will be implemented, revise the Proposed Regulations to address specific topics set out in the statute, and promote consumer education about the role of opt-out mechanisms and their limits.

3. ***Agency Audits.*** The 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 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 Proposed Regulations. Accordingly, the Proposed Regulations should explicitly state that audits will be conducted when there is a "significant risk" of violation of the CPPA and that such audits will be conducted remotely (absent specific circumstances warranting an on-site audit).

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.

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

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

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

this obligation on companies that decide how and why to collect consumers' data – rather than the service providers acting on behalf of such companies. For example, under the CCPA consumers may:

- Access personal information, by "request[ing] that a ***business*** that collects personal information about the consumer disclose" certain information to the consumer, including the "specific pieces of personal information it has collected about that consumer."[4]
- Correct personal information, by "request[ing] that a ***business*** that maintains inaccurate personal information about the consumer [] correct that inaccurate personal information."[5]
- Delete personal information, by "request[ing] that a ***business*** delete any personal information about the consumer which the business has collected from the consumer."[6]

The CCPA recognizes that service providers are not required to respond to consumer rights requests submitted to them by individuals – and for good reason. Under the statute, consumers are to exercise their rights by going to the consumer-facing company they interact with – the business – instead of forcing consumers to identify the dozens or more service providers that each consumer-facing business may utilize. This is both efficient for consumers and an important reflection of the role of service providers, which process data on behalf of other businesses and generally do not interact with individual consumers. Indeed, a service provider often lacks the information needed to identify an individual who submits a rights request – and does not make the types of decisions required to fulfill a request, which require determining the data sets to be provided to a consumer in response to a request to access personal information, assessing whether information a consumer seeks to correct is inaccurate, and analyzing whether information a consumer seeks to delete is subject to a statutory exception, such as when data is subject to a legal hold. Under the statute:

- For deletion requests, a service provider is "not [] required to comply with a deletion request submitted by the consumer directly to the service provider . . . to the extent the service provider . . . has collected, used, processed, or retained the consumer's personal information in its role as a service provider or contractor to the business."[7]
- For access requests, a service provider "shall not be required to comply with a verifiable consumer request [for access] received directly from a consumer or a consumer's authorized agent" but instead shall "provide assistance to [the] business" in responding to that request.[8]
- For requests to limit the use of sensitive personal information, a service provider is "only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business."[9]

Of course, consumer rights created by the CCPA must be meaningful in practice – including when a business engages service providers to process personal information on its behalf. That is why the CCPA creates a clear set of obligations for service providers when consumer rights requests involve data held by a service provider. Under the statute, service providers are to either: (1) respond to consumer rights requests sent to the service provider by a

[4] Cal. Civ. Code § 1798.110(a) (emphasis added).
[5] Cal. Civ. Code § 1798.106(a) (emphasis added).
[6] Cal. Civ. Code § 1798.105(a) (emphasis added).
[7] Cal. Civ. Code § 1798.105(c)(3).
[8] Cal. Civ. Code § 1798.130(a)(3)(A).
[9] Cal. Civ. Code § 1798.121(c).

business, or (2) *enable the business to respond* to those requests. The statute's clear approach – and its recognition of two ways that service providers may assist businesses in responding to requests – is critical to ensuring that companies can fully and efficiently respond to consumer rights requests. Under the CCPA:

- For a deletion request, the role of a service provider is to "cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, [to] delete, *or enable the business to delete*" information.[10]
- For access and correction requests, the role of a service provider is to "provide assistance to a business," including "providing to the business the consumer's personal information in the service provider['s] . . . possession," "correcting inaccurate information," or "*enabling the business* to do the same."[11]

The CCPA therefore recognizes that 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. Without such scalable tools, businesses would be forced to forward large volumes of consumer rights requests to service providers one-by-one. That can create a long backlog of requests, slowing down response times and creating the potential for long back-and-forth communications between the two companies about whether each request should be executed.

The Proposed Regulations do not fully account for – and at times contradict – the statute's clear recognition that service providers can fulfill their obligation to assist businesses in responding to consumer rights request by *enabling the business* to respond to those requests. For example, for correction requests Section 7023 of the Proposed Regulations appropriately recognizes that the role of a service provider is to either "comply with the business's instructions to correct the personal information *or enable the business* to make the corrections."[12] However, at least three provisions in the Proposed Regulations do not acknowledge the statute's recognition that service providers can "enable" a business to respond to requests and instead could be read to presume that the only role for a service provider is to respond to each individual consumer rights request forwarded to it by a business. Those provisions are:

- Section 7022(c), which sets out obligations for service providers after being notified of a consumer's deletion request.[13] This provision disregards the clear statutory language stating a service provider may fulfill its obligation to assist the business either by deleting the relevant personal information "or [by] enabl[ing] the business to delete" that information.[14]
- Section 7024(i), which sets out obligations for service providers for requests to access information. Although this provision recognizes the role of a service provider is to "provide assistance to the business" in responding to requests, it goes on to

[10] Cal. Civ. Code § 1798.105(c)(3) (emphasis added).
[11] Cal. Civ. Code § 1798.130(a)(3)(A) (emphasis added).
[12] Proposed Regulations § 7023(c) [hereinafter Prop. Reg.] (emphasis added).
[13] Prop. Reg. § 7022(c).
[14] Cal. Civ. Code § 1798.105(c)(3).

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

state that a service provider is to assist a business "including by providing the business the consumer's personal information it has in its possession that it obtained as a result of providing services to the business," without clearly stating the service provider may fulfill its obligation by enabling the business to access the information.[15]

- Section 7051(a)(10), which sets out new requirements for contracts between businesses and service providers, including requiring a business to inform a service provider of "any consumer request made pursuant to the CCPA that they must comply with, and provide the information necessary for the service provider . . . to comply with the request."[16] This provision appears to start from the assumption that service providers will directly respond to consumer rights requests – disregarding the clear statutory language that service providers may fulfill their obligations by enabling a business to respond to such requests.

Recommendation: The Proposed Regulations should be 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 three revisions:

1. For deletion requests, Section 7022 should be revised in two ways:

   - First, 7022(c) should be revised to state: "A service provider or contractor shall either enable the business to comply with the consumer's request to delete their personal information or, upon notification by the business comply with the consumer's request to delete their personal information by"

   - Second, 7022(b)(2) should be revised to state that a business is to comply with a consumer's request to delete personal information by: "Either deleting personal information processed on behalf of the business by its service providers or contractors if enabled to so do in accordance with 7022(c), or notifying the business's service providers or contractors to delete from their records the consumer's personal information obtained in the course of providing services; and"

2. For requests to access, Section 7024(i) should be revised to state: "A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to know, including by providing the business the consumer's personal information it has in its possession that it obtained as a result of providing services to the business, or by enabling the business to access that personal information."

3. Finally, Section 7051(a)(10) should be eliminated, because it presumes that service providers will respond to requests one-by-one rather than enabling businesses to comply directly. If the provision is retained, however, it should be revised to reflect that a service provider may either enable a business to respond to requests or may respond to individual requests upon notice by the business. For example, it could be revised to state: "Require the service provider or contractor to either enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must

[15] Prop. Reg. § 7024(i).
[16] Prop. Reg. § 7051(a)(10).

> comply with, and provide the information necessary for the service provider or contractor to comply with the request."

B. The 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.[17] 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.

However, the Proposed Regulations create contractual requirements that go beyond those in the statute, in at least three ways.

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

First, Section 7051 of the 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 received from, or on behalf of, 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 assessments, audits, or other technical and operational testing at least once every 12 months.[18]

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

---

[17] 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."

[18] Prop. Reg. § 7051(a)(7).

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."[19] 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."[20]

Section 7051 of the 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 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 reach agreements that determine which "reasonable and appropriate steps" are suitable in the context of a given service. The Proposed Regulations should be revised to avoid suggesting otherwise.

Recommendation: Section 7051(a)(7) of the 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 received from, or on behalf of, 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 assessments, audits, or other technical and operational testing at least once every 12 months.~~"

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

Second, Section 7051(a)(2) of the Proposed Regulations requires service provider contracts to "[i]dentify the specific business purpose(s) and service(s) for which the service provider . . . is processing personal information . . .."[21] It goes on to state that "[t]he business purpose or service shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific."[22]

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

[19] Cal. Civ. Code § 1798.100(d)(3).
[20] Cal. Civ. Code § 1798.140(ag)(1)(D) (emphasis added).
[21] Prop. Reg. § 7051(a)(2).
[22] *Id.*

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 service providers.

Recommendation: Section 7051(a)(2) of the Proposed Regulations should be revised to be consistent with the CCPA, as follows: "Identify the specific business purpose(s) ~~and service(s)~~ for which the service provider or contractor is processing personal information on behalf of 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 or service shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.~~"

3. Section 7051(a)(8) of the Proposed Regulations goes beyond the statute in creating a specific time period for notifying businesses about compliance.

Under the CCPA, service provider contracts must include a requirement for the service provider to inform the business if it can no longer comply with its obligations under the CCPA.[23] The statute is silent on the time period for the service provider to issue such notice. By not prescribing a specific time for notification, businesses and service providers are permitted to contractually determine the appropriate approach to notice, taking into account the specific context of each business-service provider relationship. However, the Proposed Regulations would eliminate this flexibility and instead require notice "no later than five business days after [the service provider] makes a determination that it can no longer meet its obligations under the CCPA and these regulations."[24]

To ensure that service providers have adequate time to correct temporary issues and gather the information necessary for notice, Section 7051(a)(8) should be revised to eliminate a specific time period for notice – as consistent with the CCPA.

Recommendation: Section 7051(a)(8) should be revised to eliminate a specific time period for notice, as follows: "Require the service provider or contractor to notify the business if ~~no later than five business days after~~ it makes a determination that it can no longer meet its obligations under the CCPA and these regulations."

C. The Proposed Regulations Should Continue to Clearly Recognize the Ability of Service Providers to Combine Personal Information.

Under the CCPA, a service provider is to be subject to a contract with certain limitations. These include prohibiting the service provider from combining certain types of personal information – but the statute expressly recognizes that service providers may combine personal information to perform business purposes under the statute, other than cross context behavioral advertising. Under the statute, the CPPA is required to issue regulations "further defining the business purposes for which service providers . . . may combine consumers' personal information obtained from different sources."[25] Section 7050 of the Proposed Regulations does so, including through Section 7050(b)(4), which recognizes that a service provider can use personal information to build or improve the quality of its services as long as it does not use the personal information to perform services on behalf of another person.

---

[23] Cal. Civ. Code § 1798.100(d)(4).
[24] Prop. Reg. § 7051(a)(8).
[25] Cal. Civ. Code § 1798.185(a)(10).

This issue is critical to service providers that offer services to business customers at scale, which rely on data collected across those business customers to protect and secure those services, facilitate research, develop artificial intelligence systems, improve their services, and serve multiple businesses working together. For example, an email service provider may be able to proactively identify accounts at risk of being hacked by analyzing and combining personal information associated with those accounts in the context of a particular threat actor. As another example, multiple academic institutions might ask a cloud storage provider to store research data from each of them – including personal information – in one joint repository. Indeed, there are many purposes for which service providers may combine personal information in a manner that benefits consumers, and are entirely unrelated to monetization.

Section 7050(b)(4) recognizes that service providers can retain, use, or disclose personal information to improve services offered at scale – and includes two illustrative examples that clarify how the Proposed Regulations are intended to work in practice. We strongly recommend the Proposed Regulations retain these examples, which clearly recognize that a service provider that offers services to multiple business customers can analyze data from each of those customers to "improve its services and offer those improved services to everyone."

Recommendation: We strongly recommend the Proposed Regulations retain the illustrative examples in Section 7050(b)(4).

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. These regulations are to be "updated from time to time" and, among other requirements, are not to conflict with "other commonly used privacy settings or tolls that consumers may employ."[26] 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.[27] The 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 of the Proposed Regulations.

Regardless of whether a global opt out mechanism is permissive or required, it is critically important that the mechanism be interoperable with other states' privacy laws and 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

[26] Cal. Civ. Code § 1798.185(a)(19)(A)(iv).
[27] *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

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. Creating an interoperable approach to global opt-out mechanisms will benefit both consumers, by creating a more user-friendly system that works across state lines, and companies, by driving investment in compliance processes that satisfy laws in multiple states and that accurately effectuate consumers' choices with respect to their data. If, however, one state develops requirements for a global opt-out mechanism that conflict with requirements in other states, consumers may be presented with multiple "global" opt-out links, which can create significant confusion.

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 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 Proposed Regulations how a business will be able to determine that a particular signal meets the regulations' requirements, 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 requirements and thus identify the mechanisms that companies should honor, but it is not clear from the Proposed Regulations that such a process is contemplated.

This rulemaking process should address these types of practical issues, with an eye toward ensuring that businesses have fair notice of the mechanisms they may use to comply with obligations under the CCPA. Companies will require time to build tools to respond to global opt-out mechanisms — and focusing on practical issues early on will help to foster the development 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. Any Global Opt-Out Mechanism Should Comply with the Requirements Enumerated in Section 1798.185(a)(19)(A) of the CCPA.

The CCPA also identifies six topics to be addressed by the CPPA's regulations on global opt-out mechanisms – many of which are not addressed in the Proposed Regulations.

For example, under the statute the regulations are to "define the requirements and technical specifications for an opt-out preference signal" and should, among other things, "[e]nsure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer," "[c]learly represent a consumer's intent and be free

of defaults constraining or presupposing that intent," "[e]nsure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ," and "[p]rovide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information."[28]

Many of these topics relate to how an opt-out mechanism will interact with mechanisms recognized by other states, which will soon be "commonly used privacy settings or tools" once Colorado and Connecticut's global opt-out mechanism requirements go into effect. The Proposed Regulations should be revised to address these issues, which will create greater clarity about how a global opt-out mechanism is to function.

Recommendation: Section 7025(b) should be revised to address the six categories of requirements set forth in Section 1798.185(a)(19)(A) of the CCPA. This section should also reflect an intent to re-evaluate the requirements and technical specifications after one year, to ensure the agency may timely review any updates that could further promote interoperability with opt-out mechanisms in other states or could further address practical issues that may arise as the global opt-out mechanism is implemented.

D. 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 (unless the consumer provides additional information to the company receiving the signal, such as by logging into an account for the company's website). 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."[29]

The Proposed Regulations provide few details about – or guardrails for – this authority. Section 7304 of the Proposed Regulations states that the CPPA "may audit a business, service provider, contractor, or person to ensure compliance with any provision of the

[28] Cal. Civ. Code § 1798.185(a)(19)(A).
[29] Cal. Civ. Code § 1798.185(a)(18).

CCPA."[30] 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 Proposed Regulations clearly state how privileged information will be handled, which should be addressed. Rather, the Proposed Regulations state only that consumer 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 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.

In particular, the 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 be required to have sufficient guardrails in place to mitigate the potentially significant privacy and security concerns. For example, an audit of a service provider that serves hundreds of business customers 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. For these reasons, the Proposed Regulations should be revised 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 conduced 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 recommend the CPPA 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 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~~."

[30] Prop. Reg. § 7304(a).

* * *

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