Comments of BSA | The Software Alliance on Regulations to Implement the California Consumer Privacy Act

BSA | The Software Alliance ("BSA") respectfully submits these comments on the development of regulations to implement the California Consumer Privacy Act ("CCPA" or "Act"). BSA is the leading advocate for the global software industry in the United States and around the world.[1] Our members are at the forefront of developing cutting-edge, data-driven services that have a significant impact on US job creation and the global economy. BSA members prioritize protecting the privacy and security of their customers' personal information. BSA strongly supports efforts to ensure a robust US privacy framework that provides increased transparency, enhances consumers' control over their personal information, safeguards their data, and enables legitimate uses of data that fuel continued innovation. We appreciate California's leadership on these important issues.

The CCPA and its regulations should maintain a strong set of privacy protection for California consumers, and thoughtfully crafted regulations that address some of the practical difficulties in implementing the law are an important means of achieving this goal. Importantly, many BSA members primarily provide services to business customers, and practical interpretations of the law that continue to distinguish between the role that a "business" and "service provider" play will help different organizations across the data ecosystem understand and implement appropriate obligations to protect consumers' privacy. These comments identify several challenges that arise from ambiguities in the CCPA's text but could be clarified through regulations. BSA's proposed clarifications would not only provide certainty for companies that must comply but also would help to establish practices that are consistent with consumers' expectations and the CCPA's purpose of strengthening consumer privacy protections. Specifically, BSA recommends that the Attorney General issue regulations that would:

- Clarify the scope of "personal information";
- Clarify that the definition of "consumer" does not apply to employees;
- Help ensure that opt-out requests are meaningful to consumers; and
- Provide guidance on consumer verification methods and responses to consumer requests.

We recognize that the legislative process to amend the CCPA is ongoing, and there are several bills under consideration that may address—at least in part—some of these issues. However, there is continued uncertainty regarding what the outcome of those deliberations will be and, in some instances, current proposals are not sufficiently comprehensive to address more granular implementation details under review by the Attorney General's office. As a result, we respectfully request your consideration of these important issues.

I. Clarify the Scope of "Personal Information" in Connection with Households and Publicly Available Information.

The CCPA provides an exceptionally broad definition of "personal information."[2] BSA requests that the Attorney General address two elements of the definition that present significant difficulties from an implementation perspective.

[1] BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] *See* Cal. Civ. Code § 1798.140(o).

A. Limit Obligations Concerning Household Information.

One set of challenges stems from including information about households in the CCPA's definition of "personal information."[3] Although the CCPA does not define "household," the term could encompass, for example, spouses, children, and roommates who share a dwelling. The purpose of considering household information to be "personal" may have been to deem Internet Protocol addresses and information associated with them to be personal information – which is something the definition does anyway.[4] This aspect of the "personal information" definition is out of step with other privacy laws and will create negative consequences for consumers and their privacy.

Specifically, it is unclear whether the right to opt out of sale applies to information about a household, rather than being limited to information about the specific consumer who makes an opt-out request. Section 1798.120 gives consumers the right to "direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information." The use of "the consumer's" to modify personal information, however, suggests that this right is also limited to information about the consumer who makes a request.

Leaving open contrary interpretations, *i.e.*, that household-level information is subject to the right to opt out of sale, would have negative consequences for consumers' privacy as well as business that must obey opt-out requests. For instance, roommates who are part of the same "household" might have quite different preferences about whether or not they want to prevent the sale of personal information. Similarly, parents might make different choices about the sale of their personal information than they make for their children.[5] If decisions about the sale of personal information apply to information that relates to an entire household, it is unclear how businesses will be able to maintain different individuals' preferences. Further, disclosure of information pertaining to other household members in connection with access and deletion requests could undermine the privacy rights of other consumers.

To address these difficulties, the Attorney General should adopt regulations clarifying that the right to opt out of sale applies only to information about the specific consumer who makes an opt-out request. In addition, BSA recommends that the Attorney General's regulations permit businesses to take reasonable measures to maintain individual-level opt-out preferences and to forbear from disclosing or deleting personal information, as necessary, to avoid implicating information that is about a household member, rather than an individual making a request.

B. Recognize That the Government's Disclosure of Personal Information Entails the Purpose of Further Dissemination and Use.

The second significant difficulty that the Attorney General could address concerns the exclusion of "publicly available" information from the definition of "personal information."[6] The exclusion is an important element of the CCPA,[7] but, unfortunately, it is beset by a lack of clarity. Under section 140(o)(2), information is "publicly available" if it "is lawfully made available from federal, state, or local government records, if any conditions associated with such information." Publicly available information, however, excludes "data [that] is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained."

---

[3] *See id.* § 140(o)(1).

[4] *See id.* § 140(o)(1)(A) (defining "Internet Protocol address" and "other similar identifiers" to be "personal information").

[5] *See* Cal. Civ. Code §1798.120(c) (requiring opt-in consent to sell information about consumers under the age of 16).

[6] *See* Cal. Civ. Code § 1798.140(o)(2) ("Personal information' does not include publicly available information.").

[7] *See id.*

Thus, the publicly available information exemption apparently requires businesses to ascertain the purpose, or purposes, for which government agencies maintain and release personal information. Releases of personal information by government agencies may have multiple purposes, not all of which are clear. In many cases, however, agencies release information in order to provide transparency and accountability through further analysis, for example, by journalists and researchers. Making businesses responsible for determining the purposes for which the government publishes information is inconsistent with the basic notion of making information publicly available in the first place.

The Attorney General should clarify that, for the purposes of the CCPA, a government agency's decision to make information available to the public demonstrates a purpose of allowing others to make use of the information for any lawful purpose. Such a regulation would be consistent with the CCPA's text as well as the broad purposes behind government policies of making information available to the public.

II. Limit CCPA Obligations as Applied to Employees.

A focus on *consumer* privacy pervades the CCPA. "Consumers" and "businesses" are fundamental terms in the Act, which does not refer to "employees" or "employers" at all. Nonetheless, the CCPA does not expressly exclude employees[8] from the definition of "consumer,"[9] and the definition of "personal information" includes "professional or employment-related information."[10] Thus, the CCPA's text suggests that employees and personal information relating to individuals acting in their capacities as employees are covered by the Act, notwithstanding that the overarching aim of the law is to protect "consumer" privacy.

If the CCPA is interpreted to include employees, many of the documents that employers routinely collect would be subject to the full array of consumer rights. These documents include CVs and resumes, evaluation and disciplinary records, payroll and tax record information, vacation and sick leave balances, and health plan and other benefits documentation. Such an interpretation will create several significant operational challenges for a wide range of businesses and employees while doing little, if anything, to promote *consumer* privacy. Some of the challenges include the following:

- *Right to Delete.* Employers need to keep employee data for payroll, to administer benefits, to guard against legal claims, and for myriad other management purposes. If a deletion request from a consumer requires the business to delete all information about that consumer in his or her capacity as an employee of the business, those functions could become impossible to administer.

  Although the CCPA provides several exceptions to the right to delete, these exceptions do not cover the full range of legitimate processing by an employer, and the catch-all exception for use "in a lawful manner that is compatible with the context in which the consumer provided the information"[11] does not sufficiently clarify that an employer could reject a deletion request.

- *Right to Opt Out of Sale.* The right to opt out of sale of personal information is incongruous in the employment setting. Although most employers do not sell employee data in the commonly

[8] This comment uses "employee" to refer to an individual acting in an employment- or business-related capacity, including as an employee, contractors, job applicant, director, officer, or agent of a business.

[9] *See* Cal. Civ. Code § 1798.140(g). Section 1798.140(g), in turn, refers to Cal. Code of Regulations, title 18, section 17014, which defines resident to "include (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose." This definition is expansive and appears to mean that any natural person with the requisite ties to California is a consumer, regardless of the nature of his or her interaction with the entity collecting and processing his or her personal information.

[10] Cal. Civ. Code § 1798.140(o)(1)(I).

[11] Cal. Civ. Code § 1798.105(d)(9).

understood meaning of that word, the CCPA's broad definition of "sell" could potentially create situations where an employer's legitimate use of an employee's data could be considered a sale under the CCPA. In the absence of clarification from the Attorney General, employers will need to scrutinize each instance in which they provide data to a vendor, such as a payroll processor, and may need to seek to modify their contracts with vendors to avoid the result where the vendor's processing could be considered a sale. These changes will add to the CCPA's compliance costs.

- *Access.* The right of a consumer to obtain personal information that a business "has collected about that consumer"[12] also presents challenges for employers. For example, employee information could be particularly sensitive during mergers or planning for personnel changes. The narrow exceptions that the CCPA provides to the access right are likely insufficient to address these and other situations that require employers to keep employment records confidential.

BSA therefore recommends that the Attorney General clarify that employees are not "consumers" under the CCPA. In so doing, it would provide certainty to businesses and their vendors, reduce compliance costs, and prevent the CCPA's consumer rights from becoming unintended means of compromising the confidentiality of employee records or deleting them altogether. Notwithstanding the clear intent of the CCPA to address consumer privacy and the overwhelming policy reasons for excluding employees from the scope of the law, if the Attorney General interprets the CCPA to cover the employment context, we request consideration of alternative mechanisms for deletion, access, and opt-out requests that apply to employees to mitigate the harmful consequences, such as those referenced above, that could arise.

III. Ensure That Opt-Out Requests Are Helpful and Meaningful to Consumers.

A. Allow Granular Opt-Out Requests.

The opt-out right under the CCPA sweeps broadly. The CCPA directs businesses to provide a means (further discussed below) allowing consumers simply "to opt-out of the sale of the consumer's personal information."[13] In many circumstances, consumers might wish to opt out of some sales of personal information while allowing others to continue, rather than making an all-or-nothing choice. Allowing businesses to present granular choices to consumers would help to avoid some of these potential consequences.

BSA recommends that the Attorney General clarify that the CCPA allows businesses to give consumers the choice to opt out of certain types of sales and does not require businesses to present all-or-nothing choices. This clarification would give businesses the flexibility to tailor opt-out choices that meet customers' expectations and provide them with greater control over their personal information.

B. Provide Flexibility for Opt-Out Link Displays.

Some of the CCPA's requirements for a "Do Not Sell My Personal Information" link may be difficult to satisfy in practice. Specifically, the CCPA requires this link to appear clearly and conspicuously on the "homepage" and in the privacy policies of businesses that sell personal information.[14] The definition of "homepage," in turn, refers to the term "online service," which is not defined and could capture a wide range of services, potentially including some businesses that do not have a consumer-

[12] Cal. Civ. Code §§ 1798.110(a)(5), (c)(5). *See also id.* § 1798.100(a).

[13] Cal. Civ. Code § 1798.135(a)(1); *see also id.* § 1798.120

[14] *See* Cal. Civ. Code §§ 1798.135(a)(1), (2); *see also id.* § 1798.140(l) (defining "homepage").

facing presence.[15] However, it may be difficult for non-consumer-facing services to satisfy all of the opt-out link standards that apply to "online services." For example, it is unclear how a company that does not provide a mobile app or other service that consumers use would meet a requirement to provide the opt-out link "before downloading the [business's] application."[16]

A separate issue is that the definition of "homepage" appears to require companies to display an opt-out link on every page on which personal information is collected.[17] Requiring the opt-out link to become effectively ubiquitous could lead to "notice fatigue" where consumers ignore it altogether, which undermines the consumer right that the CCPA provides.

To address these challenges, BSA recommends that the Attorney General issue regulations clarifying the obligations of businesses that do not have direct relationships with consumers regarding the opt-out link.[18] These regulations could, for example, clarify that an "online service" is one that is directed to consumers and provide that it is sufficient for businesses that are not consumer-facing to disclose a point of contact to address consumers' questions and provide a link to their privacy policies or other educational materials. With respect to placement of the opt-out link, the Attorney General should consider regulations that give businesses the flexibility to place the link in locations in which consumers are likely to find it, based on the nature of their services and how consumers use them.

C. Provide Guidance on Consumer Verification Methods and Responses to Consumer Requests.

Implementation of the CCPA's verifiable consumer request requirements must balance several objectives. On one hand, it should be easy for consumers to make access, deletion, and opt-out requests.[19] On the other hand, the inadvertent deletion or disclosure of personal information to someone other than the consumer presents a wide range of risks; consumer verification methods should provide adequate safeguards against these risks and should not require businesses to collect and process sensitive personal information solely to support verification.[20] Moreover, verification methods must be reasonable in light of the sensitivity of the information at issue, the capabilities of available technologies, and the costs to implement them.[21]

Businesses will also confront the challenge of responding to consumers who cannot be verified. Although the CCPA does not require a business to provide access to or delete personal information when the business cannot verify a consumer,[22] it does not provide further detail about the form that a response should take in such a situation.

---

[15] *See* Cal. Civ. Code §1798.140(l).

[16] *See id.*

[17] *See* Cal. Civ. Code § 1798.140(l), which states that "'[h]omepage' means the introductory page of an Internet Web site *and* any Internet Web page where personal information is collected" (emphasis added).

[18] Section 1798.185(a)(4) requires the Attorney General to establish rules and procedures governing opt-out requests.

[19] *See* Cal. Civ. Code § 1798.185(a)(7) (providing that verification methods should "minimiz[e] the administrative burden on consumers").

[20] *See id.* (listing other factors for the Attorney General to consider when developing regulations governing verification for responses to requests under sections 1798.110 and 1798.115).

[21] *See id.*

[22] *See* Cal. Civ. Code § 1798.140(y).

BSA urges the Attorney General to issue regulations that address these issues. Specifically, BSA recommends the following elements of regulations governing consumer verification and responses to verified consumer requests:

- *Flexibility in Verification Methods.* Imposing uniform or inflexible requirements for verifying consumers is unlikely to balance the objectives of verification – providing an uncomplicated way for consumers to exercise their rights and to protecting consumer privacy. Accordingly, the Attorney General's regulations should provide businesses with sufficient flexibility to determine which technologies are best suited to their data practices and consumers' expectations. At the same time, the Attorney General should clarify that requests made under the CCPA should come directly from consumers; and consumers may not use third parties to submit requests on their behalf, unless expressly authorized by the law.[23] A third party's presence would make consumer verification difficult in many circumstances and would create a wide range of privacy and security risks.

- *Responsibility of Businesses to Handle Consumer Requests.* Across a wide range of circumstances, businesses have direct relationships with consumers. As a result, businesses are in the best position to receive, evaluate, and respond to consumer requests under the CCPA, and consumers should submit their requests to the relevant business. However, in at least once instance, the CCPA introduces an ambiguity into this sensible scheme. Specifically, Section 1798.105(d) lists circumstances under which a "business *or a service provider* shall not be required to comply with a consumer's request to delete the consumer's personal information . . ." (emphasis added). This language suggests that a consumer may submit deletion requests to service providers, and that service providers may be responsible for determining whether the consumer's information is subject to any of the exceptions.

  The Attorney General should clarify that Section 1798.105 in particular, and the CCPA as a whole, calls for consumers to submit requests directly to businesses and not to service providers. Such a clarification would be consistent with the overall structure and intent behind the CCPA's consumer rights provisions.[24] In addition, many service providers may not have sufficient information to verify consumers who make requests. Interpreting the CCPA to allow consumers to submit requests to service providers could result in many consumer requests being denied because service providers are unable to verify the consumer.

- *Direction to Interact with Account Holders.* Although a business may not require a consumer "to create an account with the business in order to make a verifiable consumer request,"[25] in many instances consumers will have accounts with the business to which they wish to direct a request. For instance, a wide variety of services allow or require consumers to register or create an account for security purposes, to make payments, or to receive personalized services, among other purposes. The CCPA invites the Attorney General to consider "a password-protected account maintained by the consumer" as a factor in a business's verification decisions,[26] but it does not provide further guidance on this issue.

  BSA suggests that the Attorney General provide further details about the kinds of accounts that businesses may consider in verification decisions. Specifically, it would be helpful to know whether a password-protected account maintained by the consumer with the business is the only

[23] *See, e.g.*, Cal. Civ. Code § 1798.135(a)(1) (providing that a link to opt out of sale must enable "a consumer, or a person authorized by the consumer" to make an opt-out request).

[24] *See, e.g.*, Cal. Civ. Code §§1798.100(a), 105(a), 110(a), 115(a), and 120(a) (setting forth rights of consumers to make requests of businesses).

[25] *See* Cal. Civ. Code § 1798.130(a)(2).

[26] *See* Cal. Civ. Code § 1798.185(a)(7).

type that can play a role in verification. Companies that are subject to the CCPA create and maintain accounts under a wide variety of circumstances, and they would benefit from a better understanding of whether and how they may use them to verify consumer requests.

- *Procedures Following Failure of Verification.* Providing clarification on how businesses should respond when they are unable to verify a consumer would benefit businesses and consumers. In particular, regulations should relieve businesses of any obligation to consider or evaluate repeated requests from a consumer for whom verification has failed during the time period relevant to the request (*e.g.*, the 12-month time period governing access requests[27]).

- *Limits on Obligations Relating to Personal Information Used to Combat Fraud.* Finally, the Attorney General should issue rules that prevent verified consumer requests from becoming vehicles to undermine fraud prevention efforts.[28] Consumers and many companies benefit from the vibrant marketplace for services to detect and prevent fraud. Information that is considered personal under the CCPA plays a key role in developing and providing these services, and the Legislature understood the longstanding and widespread recognition of the importance of using personal information to combat fraud.[29] For instance, Section 1798.105(d)(2) expressly exempts from the right of deletion personal information that is used or maintained to detect or protect against fraud and a variety of other harmful activities. BSA also recognizes that a statutory amendment under consideration would allow the sale of personal information to detect fraud, security incidents, and other harmful conduct.

  These statutory limits, however, are insufficient to prevent malicious actors from using the CCPA to obtain information that could compromise fraud detection and prevention efforts. In some situations, the mere fact that a business that provides fraud detection services has information about a specific consumer could reveal how its detection systems are designed or how they operate. For example, a fraud detection company's possession of a specific email address or IP address could indicate that a specific consumer has been identified as participating in potentially fraudulent activity. In addition, if the CCPA is interpreted to require highly granular disclosures about the categories of sources and recipients of personal information, malicious actors could use the CCPA to gain valuable information about the entities that provide information to the fraud detection service or that use its services.[30] The CCPA does not appear to provide a clear ground for the business to deny verified consumer requests for these types of information.[31]

  BSA therefore recommends that the Attorney General issue regulations to clarify that businesses do not need to provide personal information to consumers or make other disclosures that are reasonably likely to compromise fraud detection and prevention efforts. The Attorney General's authority to issue such regulations includes the obligation to consider "security concerns" when developing rules governing verifiable consumer requests and discretion to adopt regulations to "further the purposes" of the CCPA.[32] Data security and cybersecurity are critical to protecting consumers' privacy. Providing businesses with the flexibility to refrain from disclosing information

[27] *See* Cal. Civ. Code § 1798.130(a)(7).

[28] This comment uses "fraud prevention" to refer to the activities identified in Cal. Civ. Code §§ 1798.105(d)(2) and 1798.140(d)(2): detecting security incidents and protect against malicious, deceptive, fraudulent, or illegal activity.

[29] *See, e.g,. Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 39 (2012) (identifying fraud prevention, including "practices designed to prevent security attacks or phishing," as a personal information practice that "would not typically require consumer choice").

[30] *See* Cal. Civ. Code §§ 1798.110(c), 115(c).

[31] *See* Cal. Civ. Code §§ 1798.100(a), (c); 1798.110(c)(5).

[32] *See* Cal. Civ. Code §§ 1798.185(a)(7), (b).

that could impair fraud prevention services would be entirely consistent with this purpose of the CCPA.

* * *

BSA supports strong privacy protections for consumers and appreciates the opportunity to provide these comments. We look forward to working with the Attorney General's Office as the rulemaking process proceeds.