Computer & Communications Industry Association
Tech Advocacy Since 1972

November 21, 2022

Via Electronic Mail (regulations@cppa.ca.gov)

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

Re: CPPA Public Comment

The Computer & Communications Industry Association ("CCIA")[1] is pleased to respond to the California Privacy Protection Agency (the "Agency" or "CPPA") Notice of Modifications to the Proposed Regulations (the "Regulations") that will implement the California Privacy Act of 2020 (the "CPRA").

INTRODUCTION

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. We support and appreciate the Agency's efforts to adopt and implement privacy regulations that will guide businesses and protect consumers. The Regulations are an impressively comprehensive set of protections and are, by far, the most developed guidelines in the nation.

These comments focus on the provisions in the proposed modifications to the Regulations ("Modified Draft Rules") that warrant revision. The aim of these suggestions is manifold. First, to ensure that the Regulations are reflective of the mandates stated in the CPRA. Secondly, the Regulations are feasible to implement in a timely and clear manner. And third, the Regulations allow flexibility in order not to inhibit innovation, which would lead to harm to businesses and consumers.

CCIA's suggested amendments to the Regulations are set forth in **Attachment A.**

[1] CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

I. GENERAL PROVISIONS

A. Restrictions on the Collection and Use of Personal Information – § 7002

The proposed modifications to § 7002 create overly prescriptive requirements that conflict with the intent of the CPRA. As highlighted by the California Privacy Protection Agency Board (the "Board") during its October meetings, the CPRA intended for this provision to provide guidance on how the requirements for this section should be understood by businesses and consumers. Purpose limitation, data minimization, and robust principles for data governance are critical and foundational elements of comprehensive privacy and data regulation. The Regulations should incorporate reasonable and proportionate standards to craft principles that balance innovation and consumer privacy.

However, the Modified Draft Rules neglect these considerations by proposing a complicated and subjective multi-factor balancing test that would apply to all collection, use, retention, and/or sharing of personal information. The highly open-ended nature of these requirements would place businesses in a constant state of uncertainty regarding whether they comply. Consumers could suffer given that a highly complex and open-ended framework would leave them with a lack of clarity regarding expectations for how their personal information will be collected, used, retained, or shared. CCIA recommends the Agency delete this multi-factor balancing test from the Regulations.

The overly narrow language in the illustrative examples could inhibit innovation. The proposed language in § 7002(b)(1) concerning the mobile flashlight application makes it clear that it should only provide flashlight services and not offer ancillary benefits that might rely on collected data—such as identifying restaurants that are too dimly lit or public areas with insufficient street lighting. This assumption—the primary function of a service should be the exclusive function—is narrower than the General Data Protection Regulation (GDPR) data minimization provision, which allows businesses to process personal information in ways that are adequate and relevant to what is necessary concerning to the purposes for which it is processed.[2] CCIA suggests the Agency clarify this language and include an example where the use of data to improve and build new features is not incompatible with the original purpose.

[2] *See* Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and

How a business uses collected data across its products and services should not be unduly limited where the privacy notice expressly discloses those potential uses and that it might occur across products/services. Consumers obtain substantial benefits from sharing data across services, such as using data from a reading app to personalize book recommendations in an online store (whether both services are offered by the same business). To avoid consumers missing from these benefits, CCIA suggests the Agency modify this consideration to clarify whether the business' use of the collected information on a different product or service is unexpected and unrelated.

Marketing and other non-privacy disclosures should not be a guiding principle in determining a consumer's reasonable expectation about the disclosures in the privacy notice. The purpose of the privacy notice is to provide a one-stop notice for consumers regarding how their data is used. Conversely, marketing materials highlight the benefits of the product or service and are not necessarily relevant to how data is used, unless the disclosure makes that connection explicit. CCIA recommends the Agency remove the marketing language in § 7002(b)(4) from the Regulations.

The proposed language in § 7002(b)(5) does not offer sufficient guidance for assessing a consumer's reasonable expectation. Consumers often lack the necessary business background to understand processor relationships or the context to reflect on how a business processes its data. To the extent this guiding principle on the degree of involvement is retained, the Regulations should be modified to focus on uses that are unexpected and offensive concerning disclosed uses.

B. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent – § 7004

When designing consumer requests and obtaining consent, businesses should be required to ensure that the language is easy to understand, that there is no manipulative or confusing language, that there is symmetry in choice, and that the methods present "easy-to-execute" options. The Regulations appropriately state that non-compliant design methods may be considered dark patterns that do not result in valid consent. But the Modified Draft Rules go beyond the CPRA and create subjective inquiries that make it difficult to operationalize for

---

Repealing Directive 95/46/EC (General Data Protection Regulation), art. 5(c), ("Principles Relating to Processing of Personal Data") 2016 O.J. (L 119) 38 (EU) [hereinafter GDPR].

businesses. For example, the revised provision still places an undue burden on design through requirements on exact symmetry in length, which might not be appropriate in all instances, and to avoid "disruptive screens." One of the key principles for consumer consent is that they are informed of their decision. Businesses should be able to inform a Consumer about the effects of their choice without it constituting a disruption or rising to the level of a dark pattern. CCIA recommends the Agency modify the Regulations to focus on prohibiting false or misleading language that could impair or interfere with a consumer's ability to exercise their choice.

II. REQUIRED DISCLOSURES TO CONSUMERS

A. Notice at Collection of Personal Information – § 7012

The Modified draft rules on third-party data collection requirements in § 7012(g)(2) are overly prescriptive for companies. Businesses often engage with various third parties for numerous services that may involve the collection of data but the focus on a physical display is disproportionate, creating an unnecessary mandate to display a physical notice despite other methods being more effective and in turn, beneficial for a consumer. For instance, if a store or restaurant employs a third-party voice assistant device that does not contain a physical display, then a notice directing the consumer to the third-party device's website should be sufficient. The Agency can look to the Federal Trade Commission (FTC) which has provided guidance for providing appropriate disclosures in various contexts through its *Dot Com Disclosures* – clarified that ensuring clear disclosure of appropriate terms based on text and available means is the more important standard upon which to rely. The FTC has made clear that using email instead of direct mail may be appropriate as long as a website operator discloses how it will provide information and provides it in a form that consumers can retain. This approach demonstrates an understanding of the need for flexibility and adaptability in creating a meaningful user experience.

The Regulations should follow a similar approach and permit notice that is "reasonable" in the context of the method of data collection. CCIA recommends the Agency modify § 7012(g)(2) to adopt the flexibility permitted by the FTC, which will enable businesses to better engage with service providers and still allow meaningful disclosures to consumers.

B. Notice of Right to Opt-Out of Sale Personal Information – § 7013

CCIA is concerned that modifications to § 7013(e)(3) exceeds the mandate of the CPRA.

This proposed modification would expand notice obligations by requiring businesses to offer an opt-out in the same manner as it discloses how data is collected, imposing heavy burdens on businesses that maintain a website but collect personal information by other means. But the CPRA only requires that the business disclose the consumer's right in its online privacy policy or on the Internet webpage.[3] The Agency has explained that the requirement seeks to address new ways in which businesses are collecting personal information and ensure that the notice is effective.[4] However, the proposed modifications would increase the burden upon businesses by no longer permitting a brick-and-mortar store to post signage directing consumers to an online notice or require a business collecting personal information over the phone to "orally" walk through the notice. In these settings, the business should have the option of "orally" directing the consumer to the website notice, as permitted for physical stores.

By way of comparison, the Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA) only require businesses to present opt-out methods clearly and conspicuously in privacy notices and readily accessible locations outside of privacy notices. These opt-outs are not required to be presented in the same manner as data collection. Adopting the approach taken in other state privacy laws, by contrast, will be beneficial to businesses and consumers as there is a clearer path forward regarding how best to provide and act upon consumer rights. A business that collects personal information outside a website should be able to satisfy its obligation by directing the consumer to its website. CCIA suggests the Agency modify the Regulation to be consistent with what is becoming the national approach and what is required by the CPRA.

The proposed modifications in § 7013(h) do not provide sufficient language specifying when the requirement to obtain opt-out consent for pre-data collection applies. The Regulations need to ensure businesses and consumers understand that the requirement will apply to data collected after the notice requirement goes into effect. CCIA recommends the Agency modify the Regulation to require affirmative consent to sell/share information collected before the opt-out notice but limiting it to information collected after the notice requirement goes into effect. These temporal specifications will align with the Regulations of privacy laws in other states,

[3] 6 CAL. CONSUMER PRIVACY ACT REGULATIONS, § 11 CCR 7021(a) (2022) § 1798.130(a)(5) [CPRA]
[4] *See* Cal. Privacy Protection Agency, Initial Statement of Reasons (Jun. 6, 2022), https://cppa.ca.gov/meetings/materials/20220608_item3_isr.pdf.

which do not prevent businesses from engaging in targeted advertising based on information already collected.

C. Alternative Opt-Out Links – § 7015

Modified Draft Rule § 7015(b) would mandate that businesses provide the opt-out icon despite it being optional under the CPRA. This new requirement may confuse consumers given that the static image looks like a toggle that a consumer can activate. This requirement also prescribes a graphic feature that may not align with a business' design layout, putting an unnecessary burden on a business without countervailing consumer benefit. CCIA recommends the Regulations do not include this requirement for an opt-out icon.

III. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

A. Request to Delete – § 7022

CCIA suggests that Agency modify § 7022(c)(4) to require "reasonable efforts" to notify third parties when the deletion is made. This would help alleviate businesses from the potential flood of requests that may come in, this delimiter would help businesses meet this requirement and, in the end, benefit the consumers.

B. Request to Correct – § 7023

The Modified Draft Rules would require a business to comply with a consumer's request to correct without any limitation. The lack of any delimiter could make this obligation overly burdensome for businesses. CCIA recommends the Agency add a "disproportionate effort" standard. This modification would prevent businesses from exerting disproportionate effort in meeting correction requests and comport with other state privacy laws that allow businesses an exemption from fulfilling requests for correction where it would be unreasonably burdensome for the controller to associate the request with personal information.[5]

C. Opt-Out Preference Signals – § 7025

[5] *See* VA. CONSUMER DATA PROT. ACT, H 2307, 2021 SPECIAL SESSION, § 59.1-577 (2022); *see also* COL. PRIVACY ACT, SB 21-190, 2021 REG. SESS., § 6-1-1307 (2022); CT. ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING, PA 22-15, 2022 Gen. Assemb., § 9(c) (2022).

By requiring that businesses recognize global opt-out preference signals, the proposed language in § 7025(b) goes beyond and contradicts what is stated in the CPRA. Section 1798.135 of the statute makes clear that businesses may choose to either provide links for consumers to opt-out of "selling," "sharing," or certain uses and disclosures of sensitive personal information; or recognize universal opt-out preference signals. Specifically, the inclusion of "if" in the CPRA reflects the clear intent that the recognition of global opt-out preference signals is to be voluntary.[6] The statute reinforces this intent in the subsequent provision through the inclusion of *allows* – "A business that *allows* consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information under paragraph (1) . . . "[7]

The Modified Draft Rules, by contrast, reject this distinction. The CPRA recognized the importance of providing businesses with this flexibility given the many uncertainties that remain concerning how such signals would be implemented, how businesses are to treat multiple global opt-out preference signals that could conflict, and how to ensure that such signals do not have anti-competitive consequences. CCIA recommends modifying Section 7025(b) to ensure the recognition of global opt-out preference signals is voluntary, to align with the CPRA. These changes should be applied throughout § 7025 to reflect that recognition of global opt-out preference signals is voluntary.

In addition, CCIA suggests that the Regulations should permit consumers to turn on and turn off the opt-out mechanism discussed in § 7025(b). The opt-out mechanism should also harmonize the treatment of that signal with the confirmatory display discussed in § 7026(g). These provisions would make the signal more user-friendly, which is a stated goal of these Regulations as indicated in § 7025(a). They would also be consistent with the treatment of cookie settings (which encompasses signals such as this) under the GDPR and Europe's ePrivacy Directive, which provide clarity that: (1) a business's website should feature a consent banner that allows visitors to either give or refuse consent to the non-necessary cookies that process personal information; and (2) methods for offering a right to refuse or requesting consent should be made as user-friendly as possible, and settings should remain available for users to revisit and

[6] "A business shall not be required to comply with subdivision (a) if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal…" CPRA, § 1798.135(b)(1)
[7] CPRA, § 1798.135(b)(2)

adjust, as they prefer.[8] Consistent treatment of signals and settings assists businesses with compliance by creating a unified, global approach.

CCIA is concerned about the scope of the requirements for businesses to process a universal opt-out mechanism ("UOOMs"). Specifically, CCIA recommends that the Agency confirm the requirements to honor UOOMs should not exceed the capabilities of eligible UOOMs that are available in the marketplace. For example, if only browser extensions can serve as UOOMs, the requirement to honor UOOM signals should only extend to browsers.

The illustrative example in §7025(c)(7)(A) appears to create unnecessary risk to consumers' privacy. The proposed language may require businesses to take extra action to associate an unauthenticated visitor with an account, which is less privacy-friendly. CCIA recommends the Regulations be modified to focus on whether the visitor is logged in to avoid any obligation for a company to process additional personal data.

D. Request to Opt-Out – § 7026

The Modified Draft Rules conflict with the statute by expanding what businesses should consider when determining the methods consumers may use to submit requests to opt-out. Instead of being limited to what is sold or shared, the Agency expands the consideration to personal information that the business "makes available to third parties." It is unclear why the Agency seeks to expand this scope, which is not aligned with Section 1798.100(d) of the statute nor consistent with the other proposed changes to the Regulations. Moreover, the modifications would add a new limitation for processing in a frictionless manner. CCIA recommends the Agency remove the added limitation for processing in a frictionless manner, especially given that the alternatives and the benefits to the consumer are unclear.

The requirement to notify third parties of a consumer's opt-out status should apply on a going-forward basis only; it should not require a company to go back to previous transactions by sending the opt-out request to all downstream partners. In any case, the notification requirement should (1) be limited only to the third parties to whom the business has sold or shared the customer's personal information, as opposed to § 7026(f)(3)'s requirement to notify all third parties with whom the business makes personal information available; and (2) include the

[8] See OFFICIAL JOURNAL OF THE EUROPEAN UNION, DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 25 NOVEMBER 2009, SECTION 20(a).

disproportionate effort standard, to prevent a business from expending unnecessary time and resources with little benefit to consumers. Indeed, while the GDPR does require notice to third parties when a consumer exercises their rights, it does not require such notice if it would require the business to expend disproportionate effort. CCIA recommends deleting §7026(f)(2).

IV. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

A. Service Providers – § 7050

The illustrative example in § 7050(b)(1) of the Modified Draft Rules purports to prohibit a form of widely accepted advertising based on email addresses. The statute permits these established practices while the basis for this proposed modification is unclear. The example would have significant implications for businesses, especially small businesses, that rely on these advertising tools to reach their customers with information that is provided to them for this purpose. A customer list that a business uploads, provided they have the necessary permission to do so and it is hashed, helps them effectively and efficiently reach their customers in a privacy-protective manner. Restricting the ability for California businesses to use such tools will make it more difficult for them to reach their customers on social media platforms, increase the costs for advertising, and disproportionately affect their ability to compete in the U.S., and global, digital markets. Especially against those competitors who operate outside the scope of the statute. CCIA's proposed modifications in Attachment A would align the example with the statute, drawing directly from the statute's definition of cross-context behavioral advertising, and avoids creating further uncertainty for businesses.

Modified Draft Rule § 7050(e) would convert all service provider or contractor relationships into third-party relationships, with a host of additional legal obligations, where the contract is not fully compliant with the Regulations. This proposal would create a disproportionate and compounding penalty when a business fails to have the required contract in place. Designating a service provider as a third party would not accurately reflect the business relationship and imposes compounding penalties by also likely necessitating a violation of the sale opt-out (which would not apply to service provider relationships). Moreover, the triggered third-party classification would not reflect the actual relationship between the business and the external party, which might be engaged in an otherwise permitted business purpose that is neither selling nor sharing. The violation of the contract provision, standing alone, would be a sufficient penalty. CCIA advises the Agency to delete this provision.

B. Contract Requirements for Service Providers and Contractors – § 7051

Section 1798.145 of the CPRA includes an exemption that exculpates businesses from a service provider and contractor non-compliance where appropriate due diligence has been conducted. CCIA encourages the Agency to provide clarity by listing factors that affirmatively indicate a violation instead of leaving businesses to formulate a reasonable belief that the external party is in violation. By listing affirmative factors, the Regulations will not place additional burdens on businesses to confirm the absence of violations. Rather, businesses will be equipped with guidance on how to best conduct due diligence, which is similar to the guidance provided to data exporters in the European Commission's Standard Contractual Clauses (SCCs). Just as the SCCs offer guidance to data exporters by instructing them that they may, "take into account relevant certifications held by the data importer" when deciding on a review or audit, the Regulations can and should also offer more clarity to businesses in this section.[9]

The language in § 7051(c) is also problematic for it creates a potential backdoor requirement that a business must conduct due diligence and audits on its service providers, contractors, and third parties. To the extent the Agency promulgates Regulations on when the exemption in section 1798.145(i) of the statute applies, they should be limited to factors that affirmatively indicate that the external party is violating its obligations – and not impose additional burdens on business to confirm the absence of violations. CCIA's suggestions in Attachment A attempt to avoid creating this risk to businesses.

C. Contract Requirements Third Parties – § 7053

The proposed requirements for this provision also create the same risks as those identified in §7051(c). CCIA suggests updating § 7053(b) to address the same aforementioned concerns and incorporate specific factors to indicate a violation instead of leaving businesses to formulate a reasonable belief that the external party is in violation.

[9] European Commission, Annex to The Commission Implementing Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679, Module 2 (8.9)(C), Transfer Controller to Processor: Documentation and Compliance, https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clausescontrollers-and-processors,

CONCLUSION

CCIA and its members thank the Agency for this opportunity to provide suggestions on how to perfect the Regulations in ways that protect consumer data, are feasible to implement, and retain flexibility for customization and innovation. The suggested alternative language discussed herein, which is also provided in **Attachment A** in redline form for ease of review, is offered as a means for achieving the best result for consumers, regulators, and the online ecosystem.

Respectfully submitted,

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue, NW, Suite 300C
Washington, D.C. 20001
amaranon@ccianet.org

November 21, 2022

ATTACHMENT A

Suggested Amendments to Proposed Rules

§ 7002(b)(3): The source of the personal information and the business's method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business's product or service, the consumer likely expects that the business will use the personal information to provide that product or service. However, the consumer may not expect that the business will use that same personal information for an unexpected and unrelated use on a different product or service offered by the business or the business's subsidiary.

§ 7002(b)(4): The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information~~, such as~~ in the Notice at Collection ~~and in the marketing materials to the consumer(s) about the business's good or service~~. For example, the consumer that receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use their phone number for the purpose of verifying the consumer's identity and not for marketing purposes. ~~Similarly, the consumer may expect that a mobile application that markets itself as a service that finds cheap gas close to the consumer will collect and use the consumer's geolocation information for that specific purpose when they are using the service~~.

§ 7002(b)(5): The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information would be unexpected and offensive ~~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 service provider if the consumer is not directly interacting with the service provider or the service provider's role in the processing is not apparent to the consumer.

§ 7004(a)(2): Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option to the extent it impairs or interferes with the consumer's ability to make a choice. Illustrative examples follow.

§ 7015(b): A business that chooses to use an Alternative Opt-out Link may ~~shall~~ title the link, "Your Privacy Choices" or "Your California Privacy Choices," and shall include the following opt-out icon adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet Homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.

§ 7025(b): A business that sells or shares personal information shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

(1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.

(2) The signal shall have the capability to indicate that the consumer has selected to turn off the opt-out preference signal.

(3) ~~(2)~~ The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

(4) The business's obligation to process a preference signal shall not exceed the technical capability of the platform, technology, or mechanism that sends the opt-out preference signal. For instance, where a signal is in an HTTP header field format, the business shall process the signal only where it is received on a browser.

§ 7025(c)(7)(A): Caleb visits Business N's website using a browser with an opt-out preference signal enabled, but he is not otherwise logged into his account. ~~and the business cannot otherwise associate Caleb's browser with a consumer profile the business maintains~~. Business N collects and shares Caleb's personal information tied to his browser identifier for cross-contextual advertising. Upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's information linked to Caleb's browser identifier for cross-contextual advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb's account information because the connection between Caleb's browser and Caleb's account is not known to the business.

§ 7026(a)(1): A business that collects personal information from consumers online, shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and at least one of the following methods—an interactive form accessible via the "Do Not Sell or Share My Personal Information" link, the Alternative Opt-out Link, or the business's privacy policy ~~if the business processes an opt-out preference signal in a frictionless manner~~.

§ 7050(b)(1): Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (*e.g.*, advertisements to women, 18-30 years old, that live in Los Angeles). The

social media company can also use a hashed customer list provided by Business S to serve Business S's advertisements to Business S's customers. However, it cannot use a list of customer email addresses provided by Business S to then target those customers with advertisements based on information obtained from other third party businesses's websites, applications, or services. ~~to identify users on the social media company's platform to serve advertisements to them.~~

§ 7050(e): ~~A person who does not have a contract that complies with section 7051, subsection (a), is not a service provider or a contractor under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with section 7051, subsection (a) may be considered a sale or sharing of personal information for which the business must provide the consumer with the right to opt-out of sale/sharing.~~

§ 7051(c): Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred nor exercises its rights to assess, audit, or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

§ 7053(b): Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.