Computer & Communications Industry Association
Tech Advocacy Since 1972

August 18, 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 Proposed Rulemaking on the Proposed Regulations (the "Regulations") that will implement the California Privacy Rights Act of 2020 (the "CPRA").

INTRODUCTION

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. We appreciate that state lawmakers have a continued interest in adopting 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 a few provisions in the Regulations that warrant revision. The aim of these suggestions is manyfold. First, to ensure that the Regulations are reflective of the mandates stated in the CPRA. Secondly, that the Regulations are

[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.

feasible to implement in a timely and clear manner. Third, that the Regulations allow flexibility in order not to not inhibit innovation. Finally, to prevent any unintended retroactive application of this new set of rules.

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

I. CONSENT AND OPT-OUT

A. Opt-Out Preference Signals – § 7025(b)

By requiring that businesses recognize global opt-out preference signals, the draft Regulations go beyond, and actually contradict, what is stated in the CPRA. Section 1798.135 of the statute makes clear that businesses may choose to either (i) provide links for consumers to opt-out of "selling," "sharing," or certain uses and disclosures of sensitive personal information; or (ii) recognize universal opt-out preference signals. The draft Regulations, by contrast, reject this approach and instead require businesses to honor global opt-out preference signals. Section 7025(b) of the draft rules should be revised to treat recognition of global opt-out preference signals as voluntary in line with the statute. *See* Attachment A.

In addition, CCIA suggests that the regulations should permit consumers to both turn on and turn off the opt-out mechanism discussed in § 7025(b). The opt-out mechanism should also harmonize treatment of that signal with the confirmatory display discussed in § 7026(f)(4).

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 treatment of cookie settings (which encompasses signals such as this) under the General Data Protection Regulation (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;[2] 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 adjust, as they prefer.[3] Consistent treatment of signals and settings assists businesses with compliance by creating a unified, global approach.

B. Appropriate Notice to Obtain Opt-Out – § 7013(e)(3)

Section 7013(e)(3) requires a business to provide a notice to opt out of data sale and data sharing in the same manner in which the business collects the personal information. The Initial Statement of Reasons (ISOR) indicates that the Agency crafted this requirement to address new ways in which businesses are collecting personal information and to ensure that the notice is effective.[4] CCIA is concerned, however, that § 7013(e)(3) exceeds the mandate of the CPRA. We suggest that this rule be more consistent with what is becoming the national approach.

The stated provisions go beyond the CPRA requirements and similar state omnibus laws. That is, Section 1798.130(a)(5) of the CPRA requires only that the business disclose the consumer's right in its online privacy policy or on the internet webpage. A business that collects personal information outside a website should be able to satisfy its obligation by directing the consumer to its website. For instance, §

---

[2] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Council Directive 95/46/EC (General Data Protection Regulation), 26 O.J. (L 119), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[3] *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).

[4] *See* Cal. Privacy Protection Agency, *Initial Statement of Reasons* (Jun. 6, 2022) [hereinafter *ISOR*], https://cppa.ca.gov/meetings/materials/20220608_item3_isr.pdf.

7013(e)(3)(A) explains that a brick-and-mortar store can post signage directing consumers to an online notice. This is less burdensome than the example in § 7013(e)(3)(B), which would require a business collecting personal information over the phone to "orally" walk through the notice. The same issue arises for connected devices in § 7013(e)(3)(C). 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 in readily accessible locations outside of privacy notices.[5] These opt-outs are not required to be presented in the same manner of data collection.[6]

If it expands notice obligations by requiring businesses to offer opt-out in the same manner as it discloses how data is collected, the Agency would impose significant burdens on businesses that maintain a website but collect personal information by other means. Adopting the approach taken in other state privacy laws, by contrast, will be beneficial to businesses and to consumers as there is a clearer path forward regarding how best to provide and act upon consumer rights. Moreover, this result would be more consistent with § 1798.130(a)(5) of the CPRA, which requires only that the business disclose the consumer's rights via online privacy policy or internet webpage.

C. Opt-Out Consent for Pre-Data Collection – § 7013(h)

As written, the Regulations do not provide language specifying when the

[5] *See* VA. CONSUMER DATA PROT. ACT, H 2307, 2021 SPECIAL SESSION, § 59.1-574(c) (2022); s*ee also* COL. PRIVACY ACT, SB 21-190, 2021 REG. SESS., § 6-1-1306 (1)(a)(III) (2022).
[6] *See id.*

requirement to obtain opt-out consent for pre-data collection applies. CCIA suggests reworking § 7013(h) to ensure that businesses and consumers understand that the requirement will apply to data collected after the notice requirement goes into effect.

More specifically, CCIA suggests that the Agency clarify § 7013(h) to require affirmative consent to sell/share information collected ***prior*** to the opt-out notice, but limiting it to information collected ***after*** the notice requirement goes into effect. These temporal specifications will align the Regulations privacy laws in other states, which do not prevent businesses from engaging in targeted advertising based on information already collected.

D. Notifying Third Parties of a Consumer's Opt-Out – §§ 7026(f)(2) and (3)

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 passing 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 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.[7]

E. Confirmation of Consumer Opt-Outs – § 7026(f)(4)

[7] *See* General Data Protection Regulation, *supra* note 2, art. 19, ("Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing").

The Regulations would require a business that sells or shares personal information to provide a means by which a customer can confirm that the business has processed their opt-out request. This new requirement appears to extend beyond the statutory requirements in the CPRA. *See* Cal. Civ. Code § 1798.120(a) & (b). Although it discusses opt-out options and mentions forthcoming regulations that will "define the requirements and technical specifications for" opt-out options, the CPRA makes no mention of the requirement to confirm processing of opt-out requests. Further, this requirement does not appear in the CDPA, CPA, Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CTDPA), the Utah Consumer Privacy Act (UCPA), or VCDPA. Such a regulation, namely, one that travels well beyond its statutory basis and other state privacy laws is a slippery slope CCIA strongly advises against.

In addition to being overly broad, the requirement to confirm the processing of opt-out requests is unnecessary. The CPRA already includes enforcement provisions that motivate businesses to honor and process consumer requests. Imposing a further obligation to confirm opt-outs seems like overkill. We note that the ISOR discloses that the Agency considered the alternative of requiring businesses to confirm receipt of opt-out requests, but determined that such a requirement was "too prescriptive."[8] Requiring opt-out confirmation would be equally prescriptive. CCIA respectfully suggests that the Agency eschew both forms of additive obligation.

The most important aspect of the Regulations is the goal of ensuring a supportive user experience. With regard to opt-out, if businesses are required to display preference, they should have the option of showing preference on their website or within

[8] ISOR, *supra* note 4, at 42.

privacy settings so that the consumer's experience is not cluttered. Enabling this type of choice furthers the Agency's desire to use a "performance-based standard that gives flexibility to the business regarding how to display the status of the consumer's request," as stated in the ISOR.[9]

II. THIRD-PARTY SERVICE PROVIDERS AND CONTRACTORS

A. The Proposed Rules Improperly Default to Converting Third Parties Into Primary Actors – § 7051(c)

Section 7051, as written, improperly converts service provider/contractor relationships into third party relationships, which imposes a host of additional legal obligations set forth in § 7052 if the contract is deemed not fully compliant with the Regulations. This language creates a double penalty whereas failure to have an appropriate contract and comply with the law holds penalty enough. This layering of additional legal exposure seems both unnecessary — the business would already have violated the contract regulations — and punitive. In addition, 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.

No other U.S. State's law creates this kind of regulatory layering. Under the GDPR, a processor is responsible for its own violation of the law. For these reasons, CCIA suggests that § 7051(c) be deleted.

B. The Rules Should Include Liability Exemptions for Violations Committed by Service Providers and Contractors – §§ 7051(e) and 7053(e)

Section 1798.145 of the CPRA includes an exemption that exculpates

[9] ISOR, *supra* note 4, at 46.

businesses from service provider and contractor non-compliance where appropriate due diligence has been conducted. As the Agency works to promulgate regulations on when this section applies, CCIA encourages it to provide added clarity by listing factors that affirmatively indicate a violation, as opposed to leaving businesses to formulate a reasonable belief that the external party is in violation. We suggest updating §§ 7051(e) and 7053(e) in order to incorporate specific factors to be considered.

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.[10]

C. The Rules Should Not Contain Overly Prescriptive Requirements for Contracts with Third Parties

The Regulations as they pertain to contracts, and specifically the provisions related to use of consumer data, third party data collection, and deadlines for providing notice of inability to comply, warrant some revision in order not to create onerous or duplicative compliance burdens that will not substantially increase privacy protections.

1. Use of Consumer Data – § 7051(a)(3)

[10] 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-clauses-controllers-and-processors, .

Section 7051(a)(3)'s requirement that contract provisions include a prohibition against using information for other purposes *in addition to* the purposes of processing seems overly prescriptive. Neither the GDPR (through SCCs) nor other state laws require contracts to include such a prohibition. Instead, they primarily require contracts with third parties to include language regarding the nature of processing, parameters around purpose, and duration; clear instructions for processing data; and both parties' rights and obligations under the agreement.[11] These laws also place confidentiality, deletion, compliance, and assessment/audit requirements on the respective parties, although these are not required to be listed in the contracts. None of these laws require contracts to include a prohibition against using information for other purposes.

2. Third-Party Data Collection – § 7012(g)(3)

Similarly, the third-party data collection requirement in § 7012(g)(3) also seems too prescriptive. The Regulations should permit notice that is "reasonable" in the context of the method of data collection. 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 Federal Trade Commission (FTC) has already provided guidance for providing appropriate disclosures in various contexts through its *Dot Com Disclosures*, which make clear that ensuring clear disclosure of appropriate terms based on text and available means is the more important standard upon which to rely.[12] For instance, the

[11] *See* VA. CONSUMER DATA PROT. ACT, *supra* note 5, § 59.1-575 (2022); *see also* COL. PRIVACY ACT, *supra* note 5, § 6-1-1305 (2022); UT. CONSUMER PRIVACY ACT, S.B. 227, 2022 Gen. Sess., § 13-61-301 (2022).

[12] *See* FTC, DOT COM DISCLOSURES: Information About Online Advertising (May 2000), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-issues-guidelines-internet-advertising/0005dotcomstaffreport.pdf.

FTC makes clear that using email instead of direct mail may be appropriate as long as a website operator discloses the manner in which it will provide information and provides it in a form that consumers can retain.[13] The FTC demonstrates an understanding of the need for flexibility and adaptability in creating a meaningful user experience. The Regulations should adopt the flexibility allowed by the FTC by permitting said third parties to provide notice in a reasonable manner. Updating § 7012(g)(3) accordingly will help to permit businesses to better engage with service providers and still allow meaningful disclosures to consumers.

D. The Deadline for Third Parties to Provide Notice of Inability Should Be Increased to Ten Business Days – § 7051(a)(8)

Section 7051(a)(8) imposes a very short period—five business days—for a service provider or contractor to notify a business it can no longer meet its obligations. According to the ISOR, the slim five-day window is "necessary so that the business can take prompt action" and will help businesses "protect consumer personal information from unauthorized use."[14] The ISOR also states that this is a reasonable and feasible maximum timeframe for service providers to provide notice.[15]

Though prompt action is important, the time period is overly burdensome. For this reason, a 10-business day window would be more appropriate and more like the Agency's past rulemaking efforts. When enacting California Consumer Privacy Act regulations, the Agency implemented a 10-business day window for businesses to acknowledge receipt of data subject access requests (DSAR).[16] Other entities provide

[13] *See id.*
[14] ISOR *supra* note 4, at 51.
[15] *Id.*
[16] CAL. CONSUMER PRIVACY ACT REGULATIONS, § 11 CCR 7021(a) (2022).

even longer notice periods, as seen with the GDPR's requirement that controllers handle DSAR requests without undue delay and "in any event within one month of receipt of the request."[17]

III. CONSUMER RIGHTS

A. Collection and Use of Consumer Data – § 7002(a)

The CPRA restricts the collection and use of personal information to what is "reasonably necessary and proportionate." Cal. Civ. Code § 1798.100(c). Section 7002(a) of the draft Regulations would implement that standard to mean "what an average consumer would expect when the personal information was collected." This interpretation somewhat alters the CPRA standard in a manner that will make implementation quite difficult.

Inserting an "average consumer" gloss on the CPRA restriction for data usage creates a mutable and subjective standard. As the mind of the "average consumer" is difficult to accurately ascertain, and consumers, businesses, and regulators may differ on what an average consumer expects, a focus on the purpose provides more clarity for businesses seeking to comply with the Regulations.

CCIA notes that the GDPR contains the same restriction as the CPRA – data usage must be limited to what is necessary in relation to the purposes for which they are processed – without adoption of an additional "average consumer" standard.[18]

B. Data Minimization – § 7002(b)(1)

The illustrative examples of data minimization practices in § 7002(b) are quite

[17] *See* General Data Protection Regulation, *supra* note 2, art. 12, ("Transparent Information, Communication, and Modalities for the Exercise of the Rights of the Data Subject").
[18] *See id.* art. 5(c), ("Principles Relating to Processing of Personal Data").

narrow. CCIA is concerned that this list will restrict innovation. For instance, the Regulations assume that the primary function of a service should be the exclusive function, an assumption more narrow than the GDPR's data minimization provision, which allows businesses to process personal information in ways that are adequate and relevant to what is necessary in relation to the purposes for which it is processed.[19] In illustrative example § 7002(b)(1), a mobile flashlight application 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. In fact, these additional features benefit the consumer. To that end, it would also be helpful for the Regulations to include an example where the use of data to improve and build net new features are not incompatible with the original purpose.

C. Correction Requests – § 7023(c)

With regard to consumer requests for correction, a "disproportionate effort" standard should apply. With the potential that tens of billions of requests will start coming in, the Agency should adopt some kind of material delimiter to this obligation.

Relieving businesses from exerting disproportionate effort in meeting correction requests would comport with other state privacy laws. The CDPA, CPA, and CTDPA allow businesses an exemption from fulfilling requests for correction where it would be unreasonably burdensome for the controller to associate the request with the personal information.[20]

This same type of delimiter should apply to the obligation in § 7022(c)(4) to notify

[19] *See id.*
[20] *See* VA. CONSUMER DATA PROT. ACT, *supra* note 5, § 59.1-577 (2022); *see also* COL. PRIVACY ACT, *supra* note 5, § 6-1-1307 (2022); CT. ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING, PA 22-15, 2022 Gen. Assemb., § 9(c) (2022).

third parties when a deletion is made. CCIA suggests that the rule be modified to require "reasonable efforts" to notify third parties.

IV. DARK PATTERNS

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 broad "symmetry in choice" standard in § 7004(a)(2) should be honed somewhat.

CCIA suggests that the Agency adopt the FTC's approach to dark patterns, which focuses on eliminating practices that are harmful rather than prescribing specific design practices that will limit innovation and creativity in design. Specifically, the FTC's enforcement policy statement forbids businesses from engaging in processes that fail "to provide clear, up-front information, obtain consumers' informed consent, and make cancellation easy."[21] The FTC does not, however, impose a requirement akin to §7004(a)(2) ("The path for a consumer to exercise a more privacy-protective option shall not be longer more burdensome than the path to exercise a less privacy-protective option"). Rather than prohibiting longer privacy-protective options, § 7004(a)(2) should adjust the requirement that *more burdensome* privacy-protective options are prohibited, rather than simply prohibiting *longer* privacy-protective options.

[21] Juliana Gruenwald Henderson, *FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions,* Federal Trade Commission (Oct. 28, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions

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,

Stephanie A. Joyce
Chief of Staff and Senior Vice President
Khara Boender
State Policy Director
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
stephaniejoyce@ccianet.org
kboender@ccianet.org

August 18, 2022

ATTACHMENT A

Suggested Amendments to Proposed Rules

§ 7002(a): A business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. ~~To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected.~~ A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with ~~what is reasonably expected by the average consumer~~ the context in which the personal information was collected. A business shall obtain the consumer's explicit consent in accordance with section 7004 before collecting, using, retaining, and/or sharing the consumer's personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.

§ 7002(b)(1): Business A provides a mobile flashlight application. Depending on the circumstances, Business A should not collect, or allow another business to collect, consumer geolocation information through its mobile flashlight application without the consumer's explicit consent because the collection of geolocation information is incompatible with the context in which the personal information is collected, i.e., provision of flashlight services. The collection of geolocation data may ~~is~~ not be ~~within the reasonable expectations of an average consumer, nor is it~~ reasonably necessary and proportionate to achieve the purpose of providing, improving, or adding features to a flashlight function.

§ 7004(a)(2): Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be ~~longer~~ more burdensome than the path to exercise a less privacy-protective option. Illustrative examples follow.

§ 7004(a)(4): Avoid manipulative language or choice architecture. The methods should not use language or wording that ~~guilts or shames~~ threatens or misleads the consumer into making a particular choice ~~or bundles consent~~ so as to subvert the consumer's choice. Illustrative examples follow.

. . .

(B) Requiring the consumer to click through false or misleading reasons why submitting a request to opt-out of sale/sharing is ~~allegedly~~ a bad choice before being able to execute their choice to opt-out is manipulative ~~and shaming~~.

(C) It is manipulative to bundle choices so that the consumer is only offered the option to consent to using personal information for reasonably expected purposes

together with purposes that are incompatible to the context in which the personal information was collected. For example, a business that provides a location-based service, such as a mobile application that posts gas prices within the consumer's location, shall not require the consumer to consent to incompatible uses (e.g., sale of the consumer's geolocation to data brokers) together with the expected use of providing the location-based services, which does not require consent. This type of choice architecture is manipulative because the consumer is forced to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business's use of personal information for unexpected or incompatible uses.

§ 7012(g)(3): A business that, acting as a third party, controls the collection of personal information on another business's premises, such as in a retail store or in a vehicle, shall also provide a notice at collection in a conspicuous manner, which takes into account the method of the data collection, at the physical location(s) where it is collecting the personal information.

§ 7013(e)(3)(B): A business that sells or shares personal information that it collects over the phone may ~~shall~~ provide notice orally during the call when the information is collected.

§ 7013(e)(3)(C): A business that sells or shares personal information that it collects through a connected device (e.g., smart television or smart watch) shall provide notice in a manner that ensures that the consumer will encounter the notice or direct the consumer to where the notice can be found online while using the device.

§ 7013(h): A business shall not sell or share the personal information it collected after the effective date and during the time the business did not have a notice of right to opt-out of sale/sharing posted unless it obtains the consent of the consumer.

§ 7022(c)(4): Notifying any other service providers, contractors, or third parties that may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. ~~If the service provider or contractor claims that such a notification is impossible or would involve disproportionate effort, the service provider or contractor shall provide the business a detailed explanation that shall be relayed to the consumer that includes enough facts to give a consumer a meaningful understanding as to why the notification was not possible or involved disproportionate effort. The service provider or contractor shall not simply state that notifying those service providers, contractors, and/or third parties is impossible or would require disproportionate effort.~~

§ 7023(c): A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected. The business shall also instruct all service providers and contractors that maintain the personal information at issue in the course of providing services to the business to make the necessary corrections in their respective systems unless such notification proves impossible or involves disproportionate effort. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections and shall also ensure that the information remains corrected. Illustrative examples follow.

§ 7025 (b): A business that elects to provide an opt-out preference signal pursuant to subdivision (b) of Section 1798.135 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.

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

~~(2)~~(3) 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) In no event should a business be expected to process a preference signal in a manner that exceeds 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): If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display ~~in a conspicuous manner~~ the status of the consumer's choice in accordance with section 7026, subsection (f)(4).

§ 7026(f)(2): ~~Notifying all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has~~

~~made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person with whom the person has disclosed or shared the personal information during that time period.~~

§ 7026(f)(3): Notifying all third parties to whom the business has sold or shared the consumer's ~~makes~~ personal information ~~available, including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises~~, that the consumer has made a request to opt-out of sale/sharing and directing them ~~1)~~ to comply with the consumer's request unless such notification proves impossible or involves disproportionate effort ~~and 2) to forward the request to any other person with whom the third party has disclosed or shared the personal information during that time period~~. In accordance with section 7052, subsection (a), those third parties ~~and other persons~~ shall no longer retain, use, or disclose the personal information unless they become a service provider or contractor that complies with the CCPA and these regulations.

§ 7026(f)(4): Providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website or its consumer privacy controls "Consumer Opted Out of Sale/Sharing" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

§ 7051(a)(3): Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any purposes other than those specified in the contract or as otherwise permitted by the CCPA and these regulations. ~~This section shall list the specific business purpose(s) and service(s) identified in subsection (a)(2).~~

§ 7051(a)(8): Require the service provider or contractor to notify the business no later than ~~five~~ ten business days after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.
~~**§ 7051(a)(10)**: Require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with, and provide the information necessary for the service provider or contractor to comply with the request.~~

~~**§ 7051(c)**: A person who does not have a contract that complies with 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 these requirements may be considered a sale for which the business must provide the consumer with the right to opt-out of sale/sharing.~~

§ 7051(e): 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(e): 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.