

From: **Lelko, Marina** [REDACTED]
To: **Regulations** <Regulations@cpga.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 23:04:48 (+02:00)
Attachments: SAFE Credit Union-CPPA Public Comment_08232020.docx (2 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good evening,

SAFE Credit Union appreciates the efforts made by the Agency to seek input from stakeholders who very much want to aid in the protection of consumer data within reasonable guardrails to succeed in compliance.

Please see our attached comments on proposed rulemaking under the CPRA of 2020. Thank you for the opportunity to comment and for considering our views.

Best,

Marina Lelko | Compliance Manager

Direct: [REDACTED]
safecu.org | Let us put YOU first.



This e-mail contains information from SAFE Credit Union and may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents is strictly prohibited. If you have received this e-mail in error, please contact the sender immediately and delete all copies. This e-mail does not create a legally binding obligation of any kind. Any rates, terms, and conditions are subject to change. See SAFE for details.

Federally insured by NCUA | Equal Housing Opportunity



August 23, 2022

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

Re: [Invitation for Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020](#)

Dear Mr. Soublet:

I am writing on behalf of SAFE Credit Union (SAFE), which serves 13 counties in Northern California. We have over 247,000 members and \$4.4 billion in assets. SAFE respectfully submits the following comments on the proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA).

As a stakeholder, SAFE is interested in providing input on rulemaking and the efforts made by the California Privacy Protection Agency (CPPA) to collect comments on new and undecided issues not already covered by the existing California Consumer Privacy Act (CCPA) regulations.

Implementation and Enforcement

As draft regulations were not published for public comment until July 8, 2022, and public hearings on the draft regulations are not scheduled until August 24-25, 2022, we respectfully request a delay of the implementation and enforcement dates. With the current implementation date of January 1, 2023, this would give businesses a very short time to review the final regulations when published and to implement all the requirements by this original implementation date. As the original enforcement date of July 1, 2023, was one year after the final regulations were supposed to be published, **SAFE recommends that the enforcement date be delayed until one year after final regulations are published.**

Language

Throughout the draft regulations, it indicates that all communications with consumers should be in straightforward, meaningful language. This contradicts with CA Civil Code 1798.130(c) requiring the use the specific terms set forth in 1798.140(v) and 1798.140(ae) for the following consumer disclosures and communications: the Notice at Collection (1798.100), responding to consumer's request to know their information (1798.110), and to know the personal information being shared (1798.115). The specific terms cited are not often straightforward or meaningful to the average consumer and so, we are left not knowing how to comply nor the appropriate language to use and reply to requests to know. **SAFE recommends the conflict in wording be resolved to align with spirit of regulation using straightforward and meaningful language.**

Sharing Exemptions

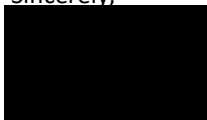
In section 7027(l), *Requests to Limit Use and Disclosure of Sensitive Personal Information*, businesses are permitted to use or disclose sensitive personal information without being required to offer consumers a right to limit for a variety of purposes such as: (1) use of information for product or services requested and (2) to detect security incidents. However, section 7026 *Request to Opt-out of Sale/Sharing* does not provide the same exemption even though the personal information being collected may be used to provide a product or service that a consumer

requested or is used by the business to detect security incidents. By not providing the same exemption, consumers will be under the false impression that they may request their personal information not be shared. In a common scenario where a vendor or third party is required to deliver the product or service, when consumers opt-out of sharing their personal information, the impact is that the financial institution will be unable to fulfill the product or service being requested. The impact may provide for a confusing consumer experience. **SAFE recommends that the same exemption afforded under section 7027(l) apply to section 7026.**

SAFE appreciates the efforts made by the CPPA to seek input from stakeholders who very much want to aid in the protection of consumer data within reasonable guiderails to succeed in compliance.

Thank you for the opportunity to comment and for considering our views.

Sincerely,



Sun Park
SVP Enterprise Risk Management & Internal Audit
SAFE Credit Union

From: **Tonsager, Lindsey** [REDACTED]
To: **Regulations** <Regulations@cpga.ca.gov>
CC: **Scott, Alexandra** [REDACTED]
Subject: CPPA Public Comment
Date: 23.08.2022 23:15:00 (+02:00)
Attachments: ESA CPRA Draft Regulations Comments (ESA FINAL 8.23.22).pdf (10 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find written comments filed on behalf of the Entertainment Software Association in connection with the CPPA's rulemaking process.

Best,
Lindsey Tonsager
Alexandra Scott
Counsel for the Entertainment Software Association

Lindsey Tonsager

Pronouns: She/Her/Hers

Covington & Burling LLP
Salesforce Tower, 415 Mission Street, Suite 5400
San Francisco, CA 94105-2533

T [REDACTED] | [REDACTED]

www.cov.com

COVINGTON



By Electronic Mail

August 23, 2022

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

Re: Written Comments on Proposed CPRA Regulations

Dear Mr. Soublet:

The Entertainment Software Association (“ESA”) submits these comments in response to the Notice of Proposed Rulemaking that the California Privacy Protection Agency (“CPPA”) published to implement the California Privacy Rights Act (“CPRA”).¹ ESA is the U.S. association for companies that produce video game consoles and publish computer and video games for video game consoles, handheld devices, personal computers, and the internet. California is home to the largest number of video game industry companies in the country, with over 400 businesses located in the state supporting more than 200,000 jobs. Accordingly, ESA appreciates the opportunity to share its perspective on the important privacy issues addressed in the CPPA’s rulemaking and the impact of the draft regulations.

ESA’s members share the CPPA’s goal of protecting the privacy and security of consumers’ personal information. For many years, ESA’s members have been leaders in providing consumers clear and understandable information about their privacy practices and developing innovative player and parental controls that enable consumers to manage their personal information online, such as online gameplay and parental consent for the collection of personal information from children. Many of ESA’s members operate globally and have decades of experience developing privacy programs in compliance with the patchwork of international data protection frameworks.

The ESA has been at the forefront of protecting children online for nearly three decades. In 1994, it founded the Entertainment Software Rating Board (“ESRB”), the non-profit, self-regulatory body that independently assigns age ratings for video games and mobile apps; educates parents about age ratings, parental controls, and privacy-related topics; enforces industry-adopted advertising guidelines; and works with major retailers to help ensure children are not sold video games rated for an adult audience without a parent or guardian present. Since 2000, the ESRB has operated ESRB Privacy Certified, an online privacy certification program to help companies in the video game industry adopt lawful, transparent, and responsible online privacy practices. That program is one of the six programs authorized by the Federal Trade Commission as a Safe Harbor under the Children’s Online Privacy Protection Act

¹ See Cal. Privacy Protection Agency, *Text of Proposed Regulations* (July 8, 2022), available at https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf [hereinafter *Draft Regulations*].

(“COPPA”). Over the decades, it has evolved to reflect changes in technology, law, and best practices for protecting consumers’ online privacy, especially for children.

Accordingly, ESA and its members have a deep understanding of how the draft regulations will impact California consumers and businesses. ESA appreciates the CPPA’s efforts to develop detailed guidance through the draft regulations with clarifying examples. However, ESA has significant concerns that:

- the draft regulations do not clearly protect California consumers and businesses against malicious and otherwise harmful activities; and
- the draft regulations also far exceed the scope of the CPRA. Certain provisions in the draft regulations are overly prescriptive and inconsistent with the CPRA’s purposes and are in tension with fundamental protections afforded by the U.S. Constitution.

Consequently, ESA requests that the CPPA revise the draft regulations to: (1) clarify that a business may deny a correction request where necessary to protect consumers or the business from malicious or harmful activities and (2) align the requirements for obtaining consumer consent with the statutory text and constitutional principles. Each of these requests is discussed in more detail below.

I. The CPPA should clarify that the correction right does not restrict a business’s ability to protect consumers from malicious or harmful activity.

The draft regulations recognize that malicious actors will use the correction right to engage in fraud and other abusive practices.² ESA appreciates that the draft regulations recognize that a business may deny such correction requests and will defer to each business’s own good-faith and reasonable belief of whether a correction request is fraudulent or abusive.³

However, the CPRA regulations could be clearer about the wide range of practices that are abusive to ensure that California consumers and business are protected from all types of malicious and harmful activity. For example, the text of the CPRA recognizes that the correction

² *Draft Regulations*, § 7023(h) (“A business may deny a request to correct if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive.”).

³ See, e.g., *id.*; CALIFORNIA PRIVACY PROTECTION AGENCY, INITIAL STATEMENT OF REASONS 31 (2022), https://cppa.ca.gov/regulations/pdf/20220708_isr.pdf [hereinafter INITIAL STATEMENT OF REASONS] (“Subsection (h) allows businesses to deny requests to correct that it has reason to believe are fraudulent or abusive, as is consistent with regulations pertaining to requests to opt-out of sale/sharing...”); Andrew Ross, *How Cyber Threats Could Grow Under GDPR*, INFORMATION AGE (May 14, 2018) <https://www.information-age.com/cyber-threats-gdpr-123472491/>; see also Martino et al., Personal Information Leakage by Abusing the GDPR “Right of Access”, USENIX (Aug. 12-13, 2019), www.usenix.org/system/files/soups2019-di_martino.pdf.

right and other consumer rights “shall not adversely affect the rights and freedoms of other natural persons,”⁴ which broadly covers any malicious or harmful activities that could impede the service functionality for other consumers or could put the privacy, security, or safety of other consumers at risk (including harassment and cheating that degrades other consumers’ gaming experiences). The CPRA also recognizes the need to protect the security and integrity of the consumer’s personal information and the service. “Security and integrity” is broadly defined to include (for example) the detection of security incidents, malicious activity, deceptive or fraudulent practices, illegal activity, or threats to consumers’ safety.⁵ Businesses also may deny correction requests that “restrict a business’ ability to . . . exercise or defend legal claims” or that are not “verifiable.”⁶ The statute is explicit that in considering whether to deny a request, the business has no legal obligation “to seek out other persons that may have or claim to have rights to personal information” or take any other action “in the event of a dispute between or among persons claiming rights to personal information in the business’ possession.”⁷ Accordingly, the implementing regulations should reflect each of these exceptions expressly set forth in the language of the CPRA.

Consistent with the CPRA’s text and intent to protect consumers and businesses from malicious or harmful activity, ESA urges the CPPA to include the following language in its regulations:

Nothing in these regulations shall restrict the ability of a business, service provider, contractor, or third party to (1) prevent, detect, protect against, or respond to fraudulent or other abusive activity, including without limitation security incidents, identity theft, fraud, harassment, malicious or deceptive conduct, or any unlawful activity; (2) investigate, report, or prosecute those responsible for any such activity or otherwise exercise or defend legal claims; or (3) ensure security and integrity. Nothing in these regulations shall require a business, service provider, contractor, or third party to take any action that adversely affects the rights and freedoms of other natural persons, seek out other persons that may have or claim to have rights to personal information, or take any other action in the event of a dispute between or among persons claiming rights to personal information in the business’ possession.⁸

⁴ Cal. Civ. Code § 1798.145(k).

⁵ *Id.* § 1798.140(ac).

⁶ *Id.* §§ 1798.145(a)(4), 1798.106(c).

⁷ *Id.* § 1798.145(k).

⁸ ESA’s proposed addition is consistent with the exemptions found in every single other state comprehensive privacy law. *See* Consumer Data Protection Act, Va. Legis. Serv. 1st Sp. Sess. 36 (2021) (West) (to be codified at Va. Code Ann. § 59.1-578(A)(7)); Concerning Additional Protection of Data Relating To Personal Privacy, 2021 Colo. Legis. Serv. Ch. 483 (West) (to be codified at Colo. Rev. Stat. § 6-1-1304(3)(a)(X)); Utah Consumer Privacy Act, 2022 Utah Laws (continued...)

II. The “dark patterns” provisions are unduly prescriptive, unsupported by the CPRA text, and in tension with fundamental protections in the U.S. Constitution.

The dark pattern provisions in the draft regulations are overly prescriptive and inconsistent with the statutory text, resulting in impractical results that are unduly restrictive and do not further the purposes of the CPRA. The provisions also are in tension with fundamental protections afforded under the U.S. Constitution.⁹ For these reasons, ESA urges the CPPA to amend Section 7004 of the draft regulations as shown in Appendix A.

A. The CPPA’s proposed dark patterns regulations are inconsistent with the language and purpose of the CPRA’s “substantial effect” standard.

The CPRA, appropriately, sets a high standard for determining that a user interface rises to the level of a manipulative “dark pattern.” It defines a “dark pattern” as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice.”¹⁰

ESA urges the CPPA to reverse Section 7004(c)’s unsupported conclusion that a user interface may be a dark pattern “regardless of a business’s intent” and requests that the CPPA limit dark patterns to deceptive and unfair practices. The Initial Statement of Reasons asserts that the CPRA’s definition does not require an “intention to subvert or impair consumer choice” (and therefore is not limited to deceptive practices) because “[w]hether a dark pattern exists

Ch. 462 (to be codified at Utah Code Ann. § 13-61-304(1)(h)); An Act Concerning Personal Data Privacy And Online Monitoring, 2022 Conn. Legis. Serv. 22-15 (West) § 10(a)(9).

⁹ The draft regulations also violate the California Administrative Procedures Act by failing to fully account for Section 7004’s adverse economic impact on industry. The CPPA grossly understated the costs and cumulative effect that Section 7004 would have on businesses as a total cost per business of \$127.50. The draft regulations vastly expand upon these existing regulations and the text of the CPRA to require businesses to completely re-engineer their opt-out mechanisms. For example, under the draft regulations a business will need to re-code the language of the choices to be symmetrical “yes” and “no” text and the colors and sizes of “yes” and “no” buttons in the consent mechanism so that they are equally prominent and symmetrical. If this language is replacing more granular choices, such as “Accept All” and “Preferences,” the business also will need to re-engineer the consent interface to create a new technical mechanism that allows the user to “Decline All” instead of selecting more granular choices consistent with their desired preferences. Businesses also will need to consider adding further clarifying language for toggles or buttons that state “on” or “off.” Depending on the mechanism, this could require re-engineering to add space for additional text. And businesses will need to eliminate all unnecessary burden or friction for the consent process, regardless of whether this burden or friction has the “substantial” effect of subverting or impairing consumer choice. The cost of re-engineering their websites and services could cost millions of dollars.

¹⁰ Cal. Civ. Code § 1798.145(l).

depends on the substantial effect of the user interface.”¹¹ This statement, however, inappropriately reads critical language out of the CPRA’s definition, which states that the user interface must be “designed or manipulated” by the business to have the substantial effect of subverting or impairing user choice. If the business does not “design” or “manipulate” the user interface to have this substantial effect, then there can be no dark pattern.¹²

Additionally, the statutory language makes clear that it is not enough for the user interface to have any or some effect. Rather, the effect must be “substantial.” Moreover, it is not enough for the user interface to exert influence over or even manipulate consumer behavior.¹³ Rather, the effect must rise to the level of “subversion” or “impairment”¹⁴ such that the consumer no longer has the ability to “self govern,” can no longer engage in “the act or process of deciding,” and no longer has the “power of choosing.”¹⁵ The implementing regulations must be consistent with the high hurdles for “dark patterns” set forth in the CPRA.

The CPPA provides no reasonable basis for how any of the activities identified in Section 7004(a) of the draft regulations satisfy the standard set forth in the CPRA. For example, Section

¹¹ INITIAL STATEMENT OF REASONS, *supra* note 3, at 13.

¹² Notably, some of the sources that the CPPA relied upon for its draft regulations recognize that dark patterns require businesses to make intentional choices. *See, e.g.,* Anuresh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites* 3 ACM HUM. COMPUT. INTERACT 81 (2019) (defining dark patterns as “user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make”) (emphasis added).

¹³ The Initial Statement of Reasons appears to treat “manipulation” of consumer behavior as a prohibited dark pattern. INITIAL STATEMENT OF REASONS, *supra* note 3, at 11 (“Accordingly, the purpose of section 7004 of these regulations is to . . . ensure that the consumer’s choice is freely made and not manipulated, subverted, or impaired.”) (emphasis added); *id.* at 12 (“This is necessary to ensure that the consumer’s choice for submitting CCPA requests and providing consent is freely made and not manipulated, subverted, or impaired through the use of dark patterns.”) (emphasis added); *id.* at 13 (“Subsection (a)(4) instructs businesses to avoid manipulative language or choice architecture [and] Subsection (a)(4)(C) is an example of how a business may bundle consent in a way that manipulates the consumer.”) However, the text of the CPRA’s “dark patterns” definition focuses on the business’s “manipulation” of the user interface, not on manipulation of consumer behavior. Accordingly, a dark pattern is plainly only that subset of user interface designs that a business manipulates to have a substantial effect of subverting or impairing user autonomy, decisionmaking, or choice.

¹⁴ *See, e.g.,* *Subverting*, MIRIAM WEBSTER ONLINE DICTIONARY, <https://www.merriam-webster.com/dictionary> (last visited Aug. 4, 2022) (defining “subverting” as “to overturn or overthrow from the foundation” or “pervert or corrupt by an undermining of morals, allegiance, or faith”); *id.* (defining “impairing” as “to diminish in function, ability, or quality”).

¹⁵ *See, e.g., id.* (defining “autonomy” as “a self-governing state”; “decisionmaking” as “the act or process of deciding something”; and “choice” as the “power of choosing”).

7004(a)(2) requires perfect “symmetry in choice.” However, there is no documented evidence in the record that asymmetry in choice inherently has a *substantial* effect of subverting or impairing the consumer’s ability to self-govern, engage in the act or process of deciding, or have the power to choose. To the contrary, a “yes” button that is in a larger size or a more eye-catching color than the “no” button still easily and readily allows the consumer to select “no.” In addition, Sections 7004(a)(4)(A)–(B) prohibit businesses from explaining the downsides of the consumer’s decision as “manipulative and shaming.” This practice of explaining the downsides of an option can, however, help ensure that the consumer’s consent is fully informed and does not prevent the consumer from self-governing, deciding, or making a free and fully informed choice. While some scholars might share the opinion that such practices are “annoy[ing]” or “frustrating,”¹⁶ these practices clearly do not satisfy the CPRA’s high standard. Further, nothing in the Initial Statement of Reasons demonstrates that any of these activities have even a *de minimis* or speculative effect, much less a “*substantial*” effect on consumer decisionmaking and choice. Accordingly, ESA requests that the CPPA remove all activities from Section 7004 that it cannot demonstrate through substantial competent and reliable evidence satisfy all elements of the CPRA’s “dark patterns” definition.

Moreover, instead of applying the CPRA’s definition of “dark patterns” to identify practices that satisfy this explicit standard, the draft regulations pull from multiple academic and research articles that purport to identify dark patterns, often in contexts other or much broader than consumer consent with respect to data privacy.¹⁷ Significantly, this scholarship applies different, and lower, standards and definitions than the CPRA for determining if an activity is a dark pattern, ranging widely from any “practices in digital interfaces that steer, deceive, coerce, or manipulate consumers into making choices that often are not in their best interests”¹⁸ to any activities that “can distort consumer behaviour.”¹⁹ This approach inappropriately substitutes the judgment of unelected scholars for the expressed will of the California electorate set forth in the text of the CPRA.

¹⁶ Anuresh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites* 3 ACM HUM. COMPUT. INTERACT 81 (2019); Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. Legal Analysis 43, 44 (2021).

¹⁷ INITIAL STATEMENT OF REASONS, *supra* note 3, at 11 (stating that the activities identified in Section 7004(a) were “informed by significant academic scholarship on the topic of dark patterns”).

¹⁸ Francisco Lupianez-Villanueva et al., European Commission, Directorate General for Justice and Consumers, *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation*, at 20 (2022).

¹⁹ *Evidence Review of Online Choice Architecture and Consumer and Competition Harm*, COMPETITION AND MARKETS AUTHORITY (April 5, 2022), <https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers/evidence-review-of-online-choice-architecture-and-consumer-and-competition-harm>.

Regulations must hew to the constraints of their implementing statute.²⁰ The proposed regulations on “dark patterns” certainly are no exception, and the CCPA should revise its proposed regulations to conform with the very specific modifiers in the CPRA’s definition of a “dark pattern.”

B. The draft regulations’ treatment of dark patterns is in tension with fundamental protections afforded by the U.S. Constitution.

The proposed dark pattern regulations raise serious constitutional concerns in multiple respects.

First, the draft regulations would chill constitutionally protected speech in violation of the First Amendment.²¹ The draft regulations’ definition of “dark pattern”²² (and efforts to define what is *not* a dark pattern)²³ are so nebulous and subjective that a business subject to the regulations could have little confidence that its user interface will be found to not have the

²⁰ California courts will not enforce, and the agency should not promulgate, a contrary regulation. *See, e.g., Colmenares v. Braemar Country Club, Inc.*, 63 P.3d 220, 225 (Cal. App. Ct. 2003) (“An agency invested with quasi-legislative power to adopt regulations has no discretion to promulgate regulations that are inconsistent with the governing statute, in that they alter or amend the statute or enlarge or impair its scope.”) (internal quotations and citations omitted); CALIFORNIA DEPARTMENT OF JUSTICE, FINAL STATEMENT OF REASONS, APPENDIX A, Row 17 (2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf> (“The OAG cannot implement regulations that alter or amend a statute or enlarge or impair its scope.”).

²¹ *See Stanley v. Georgia*, 394 U.S. 557, 564(1960); *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 566 (2011) (“Lawmakers may no more silence unwanted speech by burdening its utterance than by censoring its content.”). Even if a website’s choices about the design of a user interface for submitting CCPA requests and granting data-related consents were “commercial speech,” *but cf. Cent. Hudson Gas & Elec. Co. v. Pub. Serv. Comm’n of N.Y.*, 447 U.S. 557, 562 (1980) (“speech proposing a commercial transaction” subject to lessened scrutiny), the First Amendment would still protect those choices to the extent they are not inherently misleading, *see id.* at 563–64 (government regulation of commercial speech must “directly advance” a “compelling” state interest). Nor can the State circumvent the First Amendment by simply redefining what speech is “misleading.” *Cf. Ocheesee Creamery LLC v. Putnam*, 851 F.3d 1228, 1238 (11th Cir. 2017). In any event, it is far from clear that the Supreme Court would agree that “commercial” speech is entitled to reduced protection. *See, e.g., 44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 517 (1996) (Scalia, J., concurring in part and in the judgment) (“*Central Hudson* test . . . seems to have nothing more than policy intuition to support it); *id.* at 522 (Thomas, J., concurring in part and in the judgment) (no “philosophical or historical basis for asserting that ‘commercial’ speech is of ‘lower value’ than ‘noncommercial’ speech”).

²² *Draft Regulations*, § 7004(c).

²³ *Id.* § 7004(a).

objective effect of “substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of [the] business’s intent.”²⁴ Faced with practically unresolvable uncertainty about whether its consumer consents will be invalidated after the fact, many businesses will simply decline to collect and use consumer data, preventing them from communicating with their users in ways that are informed by and tailored to those users’ interests and preferences.²⁵

Additionally, the regulations require businesses to avoid “manipulative”²⁶ language and choice architecture. Despite these broad requirements, however, the CPPA provides only “illustrative” examples of prohibited or acceptable conduct.²⁷ For example, the regulations impose content-based restrictions on speech that is not inherently misleading, prohibiting businesses from making truthful and protected statements to consumers like “No, I don’t want to save money” or “No, I like paying full price.”²⁸ Therefore, it will be nearly impossible for businesses to assess whether any alternatives outside of the handful of examples provided in the regulations are “manipulative” and “confusing.” Thus, the regulations force businesses to self-censor and use only that language and formatting that is the most unobjectionable. Moreover, the regulations impose content-based restrictions on speech, prohibiting businesses from making truthful and protected statements to consumers.²⁹ Suppressing such speech does not further any legitimate state interest and cannot survive First Amendment scrutiny.

Second, the draft regulations’ treatment of dark patterns also raises void-for-vagueness concerns under the Due Process Clause of the Fourteenth Amendment.³⁰ As discussed above, the regulations leave industry members unsure as to what consumer consent mechanisms the CPRA does and does not permit.

Third, the draft regulations likely violate the Dormant Commerce Clause. The Commerce Clause authorizes Congress “[t]o regulate Commerce with foreign Nations, and among the several States.”³¹ This affirmative grant of authority to Congress also encompasses an implicit or “dormant” limitation on the authority of the states to enact legislation “that

²⁴ *Id.* § 7004(c).

²⁵ *Reno v. Am. C.L. Union*, 521 U.S. 844, 872 (1997) (“The vagueness of the CDA is a matter of special concern for two reasons. First, the CDA is a content-based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech.”).

²⁶ *Draft Regulations*, § 7004(a)(4).

²⁷ *Id.* § 7004(a)(2)–(4).

²⁸ *Draft Regulations*, § 7004(a)(4).

²⁹ *Draft Regulations*, § 7004(a)(4).

³⁰ *Sessions v. Dimaya*, 138 S. Ct. 1204, 1212 (2018) (“The void-for-vagueness doctrine, as we have called it, guarantees that ordinary people have ‘fair notice’ of the conduct a statute proscribes.”).

³¹ U.S. Const. art. I, § 8, cl. 3.

California Privacy Protection Agency
 August 23, 2022
 Page 9

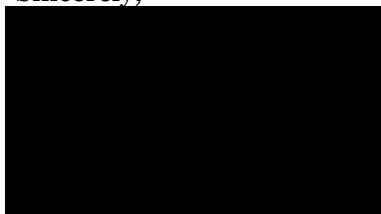
discriminates against or unduly burdens interstate commerce and thereby ‘imped[es] free private trade in the national marketplace.’”³² A state law might “unduly burden[] interstate commerce” if it practically requires out-of-state commerce to be conducted at the regulating state’s direction.”³³ Many of the technical specifications set forth by Section 7004 are far more onerous than those contemplated by similar state laws³⁴ or FTC guidance.³⁵ Due to the difficulty of establishing geographic boundaries across the internet, Section 7004 appears to reach activity outside of California in violation of the Dormant Commerce Clause.³⁶

For each of the reasons described above, ESA urges the CPPA to amend Section 7004 as indicated in Appendix A. These edits will also facilitate compliance and provide businesses with a better understanding of how the law regulates complicated consent frameworks. In turn, businesses will be able to tailor their consent frameworks to particular interactions with users (e.g., using language that is appropriate for the particular context while still empowering consumers to exercise effective choices).

* * *

ESA appreciates the CPPA’s considerations of these comments, and we look forward to continuing to work with the CPPA on these important issues.

Sincerely,



Maya McKenzie
 Counsel, Technology Policy
 Entertainment Software Association

³² *Gen. Motors Corp. v. Tracy*, 519 U.S. 278, 287 (1997) (emphasis added) (internal citations omitted).

³³ *See, e.g., Brown-Forman Distillers v. N.Y. State Liquor Auth.*, 476 U.S. 573, 582 (1986).

³⁴ *See An Act Concerning Personal Data Privacy And Online Monitoring*, 2022 Conn. Legis. Serv. 22-15 (West) §§ 12(1), (11) (incorporating the FTC’s standard).

³⁵ *See supra* notes 7–10 and accompanying text.

³⁶ *Harley-Davidson, Inc. v. Franchise Tax Bd.*, 187 Cal. Rptr. 3d 672, 680 (Cal. Ct. App. 2015) (“[A] discriminatory regulation must be invalidated unless its proponent can “show that it advances a legitimate local purpose that cannot be adequately served by reasonable nondiscriminatory alternatives.”) (internal citations omitted).

Appendix A

ESA's Proposed Edits to Section 7004 of the Draft Regulations

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

- (a) Businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that use language that is easy for consumers to read and understand. When applicable, they shall comply with the requirements for disclosures to consumers set forth in section 7003.
- (b) A business that designs or manipulates its user interface as follows will be deemed to have the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice:
 - (1) A choice in buried language that obscures disclosures and material terms.
 - (2) A choice using poorly labeled hyperlinks that hide material terms from consumers.
 - (3) A choice using trick language that confuses consumers.
 - (4) A choice using bait and switch practices.
 - (5) A choice that uses language or interactive elements that are deceptive or unfair.
 - (6) A choice that uses double negatives. Toggles or buttons must clearly and truthfully reflect the consumer's choice. Illustrative examples follow.
 - (A) Giving the choice of "Yes" or "No" next to the statement "Do Not Sell or Share My Personal Information" is a double negative and a confusing choice for a consumer.
 - (B) Toggles or buttons that state "on" or "off" may be confusing to a consumer and may require further clarifying language.
 - (C) Unintuitive placement of buttons to confirm a consumer's choice may be confusing to the consumer. For example, it is confusing to the consumer when a business at first consistently offers choices in the order of Yes, then No, but then within the same screen or page offers choices in the opposite order—No, then Yes—when asking the consumer something that would benefit the business and/or contravene the consumer's expectation.
- (5) Easy to execute.
 - (A) Upon clicking the "Do Not Sell or Share My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.
 - (B) Circular or broken links, and nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this regulation.
 - (C) Businesses that require the consumer to unnecessarily wait on a webpage as the business processes the request may be in violation of this regulation.

From: **Saul Bercovitch** [REDACTED]
To: **Regulations** <Regulations@cpga.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 23:26:44 (+02:00)
Attachments: CCPA Rulemaking CLA Privacy Law Section Comments - 8-23-22 (FINAL).pdf (19 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

I have attached comments of the Privacy Law Section of the California Lawyers Association on the proposed regulations implementing the California Consumer Privacy Act that were provided for public comment beginning on July 8, 2022. Thank you.

Saul Bercovitch | Director of Governmental Affairs

California Lawyers Association

[400 Capitol Mall, Suite 650 | Sacramento, CA 95814](#)

O: [REDACTED] | [REDACTED]



PRIVACY LAW



CALAWYERS.ORG/PRIVACY

August 23, 2022

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

Sent via e-mail to regulations@coppa.ca.gov

Re: *Comments to July 8, 2022 Proposed California Consumer Privacy Act Regulations*

Dear Mr. Soublet:

The Privacy Law Section of the California Lawyers Association ("CLA") respectfully submits its comments on the proposed regulations implementing the California Consumer Privacy Act ("CCPA") that were provided for public comment beginning on July 8, 2022.

CLA is the statewide bar association for California lawyers. It has approximately 72,000 members and is one of the largest statewide voluntary bar associations in the United States. CLA's mission is to promote excellence, diversity, and inclusion in the legal profession and fairness in the administration of justice and the rule of law. CLA has 18 sections that focus on specific areas of subject matter expertise.

The Privacy Law Section has over 800 members and represents a multidisciplinary group of privacy practitioners including consumer privacy advocates, government regulators, law firm practitioners, chief privacy officers, in-house privacy counsel, and policy analysts at privacy think tanks. Our members have broad-ranging expertise in areas that include consumer privacy, cybersecurity, and data protection, with experience in related regulatory, transaction, and litigation matters.

The comments submitted by the Privacy Law Section use the following format: 1) we quote the rule as proposed by the California Privacy Protection Agency ("Agency"); 2) we provide our comment regarding the proposed rule; and 3) we propose revisions to the proposed rule consistent with our comment, using strikeouts for proposed deletions and underlines for proposed additions.

Article 1. GENERAL PROVISIONS

§ 7001. Definitions.

Rule

§ 7001(h). “Disproportionate effort” within the context of a business responding to a consumer request means the time and/or resources expended by the business to respond to the individualized request significantly outweighs the benefit provided to the consumer by responding to the request. For example, responding to a consumer request to know may require disproportionate effort when the personal information which is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and would not impact the consumer in any material manner. In contrast, the benefit to the consumer of responding to a request to correct inaccurate information that the business uses and/or sells may be high because it could have a material impact on the consumer, such as the denial of services or opportunities. Accordingly, in order for the business to claim “disproportionate effort,” the business would have to demonstrate that the time and/or resources needed to correct the information would be significantly higher than that material impact on the consumer. A business that has failed to put in place adequate processes and procedures to comply with consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer’s request requires disproportionate effort.

Comments

The Privacy Law Section has two concerns about this proposed definition. First, the proposed standard is unworkable in practice and could lead to the erosion of privacy rights. Second, the requirement for businesses to have “adequate processes and procedures” in order to use the disproportionate effort defense creates uncertainty for business as to what is considered adequate.

The proposed standard invites uncertainty and potential invasions of privacy. By requiring a business to consider the potential benefits to the *individual* consumer in responding to the individualized request, the proposed standard invites invasive questions or presumptions by the business relative to the individual consumer. In practice, this standard may lead a business to either: (a) question the consumer about the particular benefit the response would provide them (which invites additional data collection or invasive questions), or (b) speculate on how the denial of a request would negatively impact a consumer about whom the business may have little to no insight or context. We believe both instances are potentially problematic and could lead to unintended consequences and an erosion of privacy, rather than a fortification of it.

Instead, the proposed standard should be based on whether the business’s effort in responding to an access or correction request outweighs the reasonably foreseeable impact to the consumer in not responding, taking into account the time and costs likely to be incurred by the business in responding, the size and revenue of the business, and the purposes for which the information is maintained by the business. This standard would allow the business to weigh the quantifiable costs and impact to the business

against non-particular but reasonably foreseeable impact to the consumer. Such a standard would allow the business to consider the sensitivity of the personal information and potential impacts to the consumer but would not require the business to conduct individualized impact assessment with respect to a particular consumer based on their request.

Second, the requirement that businesses implement “adequate” processes and procedures as a condition for claiming disproportionate effort creates uncertainty about the adequacy of common CCPA compliance practices and efforts by the business to comply with some of the more challenging aspects of the CCPA. Instead of requiring a separate process to determine the adequacy of a process for claiming disproportional effort, we suggest amending the requirement to require only that the business have adequate processes and procedures in place to receive and process consumer requests in accordance with the CCPA and the implementing regulations.

Proposed Alternative Language

§ 7001(h). “Disproportionate effort” within the context of a business responding to a consumer request means the time and/or resources expended by the business to respond to the individualized request significantly outweighs the reasonably foreseeable impact to the consumer by not responding, taking into the account the size of the business, the nature of the request, the technical limitations impacting the ability to respond, and other applicable circumstances.~~benefit provided to the consumer by responding to the request.~~ For example, responding to a consumer request to know may require disproportionate effort when the personal information which is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and there is no reasonably foreseeable material impact to the consumer by not responding.~~would not impact the consumer in any material manner.~~ In contrast, the impact ~~benefit~~ to the consumer of denying ~~responding to~~ a request to correct inaccurate information that the business uses and/or sells may outweigh the burden on the business in honoring the request when the reasonably foreseeable consequence of denying the request would be be high because it could have a material impact on the consumer,~~such as the denial of services or opportunities to the consumer.~~ Accordingly, ~~in order for the business to claim “disproportionate effort,” the business would have to demonstrate that the time and/or resources needed to correct the information would be significantly higher than that material impact on the consumer.~~ A business that has failed to put in place adequate processes and procedures to receive and process ~~comply with~~ consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer’s request requires disproportionate effort.

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

Rule

§ 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. 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.

Comments

Section 7002(a) proposes that a business "shall obtain the consumer's explicit consent...before collecting, using, retaining, and/or sharing the consumer's personal information for any purpose that is unrelated or incompatible with the purpose for which the personal information [was] collected or processed." The obligation by a business to obtain explicit consent to collect or process personal information is not included in the text of the CCPA statutory amendments and appears to be inconsistent with the plain language of the statute.

Civil Code section 1798.100(a)(1) states that unrelated or incompatible uses of personal information are prohibited without providing additional *notice* to the consumer. ("A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with *notice* consistent with this section." (emphasis added)).

The statute does not include a general right to opt into the collection of personal information; indeed, the statute provides that right only in specific circumstances, such as consent for the sale of a child's personal information. The Privacy Law Section recommends the Agency remove the explicit consent requirement and return to the language of the statute, Civil Code section 1798.100(a)(1), that requires notice be provided when businesses collect or use personal information for unrelated or incompatible purposes. To the extent that this change would require modification or deletion of the examples set forth in subsection (b), we suggest making such changes. Also, to the extent the Agency accepts the recommendation of the Privacy Law Section with respect to subsection (a), we do not believe that subsection (c) needs amendment.

Proposed Alternative Language

§ 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. A business shall provide notice ~~obtain the consumer's explicit consent~~ in accordance with section 7012 ~~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.

ARTICLE 2. REQUIRED DISCLOSURES TO CONSUMERS

§ 7012. Notice at Collection of Personal Information.

Rule

§ 7012(a). The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, the purposes for which the personal information is collected or used, and whether that information is sold or shared, so that consumers can exercise meaningful control over the business's use of their personal information. Meaningful control in this context means to provide consumers with the opportunity to choose how to engage with the business in light of its information practices. For example, upon receiving the notice at collection, the consumer should have all the information necessary to choose whether or not to engage with the business, or to direct the business not to selling or sharing [*sic*] their personal information and to limit the use and disclosure of their sensitive personal information.

Comments

Section 7012(a) states that the purpose of the notice at collection is to provide consumers with "meaningful control" over the business's *use* of their personal information. Section 7012(a) goes on to clarify that the notice at collection should include "all the information necessary to choose whether or not to engage with the business...." The Privacy Law Section suggests that "meaningful control" must be understood in the context of the existing rights afforded by the CCPA. The CCPA does not provide consumers the right to prohibit the collection or use of personal information outright, as the "whether or not to engage with the business" language implies. Instead, we posit that meaningful control is properly understood to mean that the consumer can meaningfully exercise their CCPA rights with the business to have meaningful control over how the personal information is used by the business.

We suggest that the Agency amend subsection 7012(a) to strike the language pertaining to "whether or not to engage" with the business. This change would clarify that upon receiving the notice, consumers have the right to exercise control over how businesses use their personal information consistent with the rights set forth in the CCPA. This interpretation of the CCPA is accurate given that the notice at collection must be provided to the consumers at or before the point of collection. This assumes that a proper notice of collection may be provided at the time personal information is being collected. If this notice is being provided at the point of collection, that means the point at which the consumer may choose whether or not to engage with the business may have already passed but the consumers still have the opportunity to direct the business not to sell or share their personal information or to limit the use and disclosure of their sensitive personal information.

In addition, we suggest the Agency correct typographical errors in subsection 7012(a) as proposed below.

Proposed Alternative Language

§ 7012(a). The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, the purposes for which the personal information is collected or used, and whether that information is sold or shared, so that consumers can exercise meaningful control over the business's use of their personal information. Meaningful control in this context means to provide consumers with the opportunity to choose how to engage with the business in light of its information practices. For example, upon receiving the notice at collection, the consumer should have all the information necessary to ~~choose whether or not to engage with the business, or to direct the business not to selling or sharing~~ their personal information and to limit the use and disclosure of their sensitive personal information.

Rule

§§ 7012(c)(4) and (5) [Proposed for Deletion by the Agency]

~~(4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just in time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just in time notice, such as through a pop up window when the consumer opens the application, that contains the information required by this subsection.~~

~~(5) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.~~

Comments

For the reasons stated in our comments to subsection 7002(a), the Privacy Law Section suggests that the Agency maintain the examples set forth in subsections 7012(c)(4) and (5). These subsections provide helpful guidance to businesses about how to provide "just-in-time" notices to consumers. They are also consistent with Civil Code section 1798.100(a), which requires additional notice to process personal information for purposes that are incompatible with the disclosed purpose for which personal information was collected.

Proposed Alternative Language

4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight

application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, that contains the information required by this subsection.

(5) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.

Rule

§ 7012(g)(1). For purposes of giving notice at collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a notice at collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a notice at collection.

Comments

Section 7012(g)(1) states that more than one business may control the collection of personal information and thus have an obligation to provide a notice at collection in accordance with the CCPA and these regulations. The rule proposes an example of a joint-controller scenario in the website context and concludes that "[b]oth the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a notice at collection." The Privacy Law Section suggests the rule clarify that, in the online context, the first party and the third party controlling the collection of personal information are not each required to provide a *separate* notice at collection.

Clarifying this language would harmonize the seemingly incongruous language between subsection (g)(1) and subsection (g)(2), which states that a first party can identify the specific third parties who control the collection of personal information, or their business practices, in the first party's notice at collection. The proposed change would be consistent with the example set forth in subsection 7012(g)(4)(A), which does not require Business G to provide a separate notice at collection on Business F's website.

Proposed Alternative Language

§ 7012(g)(1). For purposes of giving notice at collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a notice at collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a notice at collection-, which may be provided in a single notice.

Rule

§ 7012(e)(6). If a business allows third parties to control the collection of personal information, the names of all the third parties; or, in the alternative, information about the third parties' business practices.

§ 7012(g)(4)(A). Business F allows Business G, an analytics business, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its notice at collection, which shall identify Business G as a third party authorized to collect personal information from the consumer or information about Business G's information practices, on the introductory page of its website and on all webpages where personal information is collected. Business G shall provide a notice at collection on its homepage.

§ 7012(g)(4)(B). Business H, a coffee shop, allows Business I, a business providing wi-fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the notice at collection for Business H can be found online. Business H's notice at collection shall identify Business I as a third party authorized to collect personal information from the consumer or include information about Business I's practices in its notice. In addition, Business I shall post its own notice at collection on the first webpage or other interface consumers see before connecting to the wi-fi services offered.

Comments

"Business practices" appears to refer to the option to describe third parties' practices instead of identifying them by name. However, this term is not used consistently throughout section 7012. When first introduced in subsection 7012(e)(6) (and in the Initial Statement of Reasons ("ISOR")), the term "business practices" is used. However, subsequent illustrative examples use the term "information practices" (subsection 7012(b)(4)(A)) and generic "practices" of a business (subsection 7012(b)(4)(B)) to reference the same concept. The Privacy Law Section suggests that this inconsistency be remedied as proposed below.

Proposed Alternative Language

§ 7012(g)(4)(A). Business F allows Business G, an analytics business, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its notice at collection, which shall identify Business G as a third party authorized to collect personal information from the consumer or information about Business G's ~~information~~business practices, on the introductory page of its website and on all webpages where personal information is collected. Business G shall provide a notice at collection on its homepage.

§ 7012(g)(4)(B) Business H, a coffee shop, allows Business I, a business providing wi-fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the notice at collection for

Business H can be found online. Business H's notice at collection shall identify Business I as a third party authorized to collect personal information from the consumer or include information about Business I's business practices in its notice. In addition, Business I shall post its own notice at collection on the first webpage or other interface consumers see before connecting to the wi-fi services offered.

Rule

§ 7012(g)(4)(C). Business J, a car rental business, allows Business M to collect personal information from consumers within the vehicles Business K rents to consumers. Business J may give its notice at collection, which shall identify Business K as a third party authorized to collect personal information from the consumer or include information about Business K's practices, to the consumer at the point of sale, i.e., at the rental counter, either in writing or orally. Business K may provide its own notice at collection within the vehicle, such as through signage on the vehicle's computer dashboard directing consumers to where the notice can be found online. Business K shall also provide a notice at collection on its homepage.

Comments

Subsection (g)(4)(C) appears to contain two typographical errors. We suggest modifications as set forth below.

Proposed Alternative Language

§ 7012(g)(4)(C). Business J, a car rental business, allows Business ~~M~~K to collect personal information from consumers within the vehicles Business ~~K~~J rents to consumers. Business J may give its notice at collection, which shall identify Business K as a third party authorized to collect personal information from the consumer or include information about Business K's practices, to the consumer at the point of sale, i.e., at the rental counter, either in writing or orally. Business K may provide its own notice at collection within the vehicle, such as through signage on the vehicle's computer dashboard directing consumers to where the notice can be found online. Business K shall also provide a notice at collection on its homepage.

§ 7013. Notice of Right to Opt-Out of Sale/Sharing and the “Do Not Sell or Share My Personal Information” Link.

Rule

§ 7013(a). The purpose of the “Do Not Sell or Share My Personal Information” link is to immediately effectuate the consumer's right to opt-out of sale/sharing, or in the alternative, direct the consumer to the notice of right to opt-out of sale/sharing. Accordingly, clicking the business's “Do Not Sell or Share My Personal Information” link will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

Comments

The words “immediately” and “immediate” add unnecessary potential confusion because opt outs may not be executed “immediately,” but could nevertheless be executed well within 15 business days without requiring consumers to take further steps, such as being redirected to a separate notice of right to opt out. Removing the reference to timing would eliminate confusion.

Proposed Alternative Language

§ 7013(a). The purpose of the “Do Not Sell or Share My Personal Information” link is to ~~immediately~~ effectuate the consumer’s right to opt-out of sale/sharing, or in the alternative, direct the consumer to the notice of right to opt-out of sale/sharing. Accordingly, clicking the business’s “Do Not Sell or Share My Personal Information” link will either have the ~~immediate~~ effect of opting the consumer out of the sale or sharing of personal information by the business, or lead the consumer to a webpage where the consumer can learn about and make that choice.

Rule

§ 7013(e)(1). ... If clicking on the “Do Not Sell or Share My Personal Information” link immediately effectuates the consumer’s right to opt-out of sale/sharing or if the business processes opt-out preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.

Comments

There may be situations where a business may not be able to immediately effectuate the consumer’s right to opt-out of sale/sharing. We recommend that the Agency allow for the business to effectuate the consumer’s right to opt-out of sale/sharing within the timeframe allotted by the statute and not add a separate requirement to immediately effectuate the consumer’s right to opt-out.

Proposed Alternative Language

§ 7013(e)(1) If clicking on the “Do Not Sell or Share My Personal Information” link ~~immediately~~ effectuates the consumer’s right to opt-out of sale/sharing or if the business processes opt-out preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.

§ 7015. Alternative Opt-Out Link.

Rule

§ 7015(b). A business that chooses to use an alternative opt-out link shall title the link “Your Privacy Choices” or “Your California Privacy Choices,” and shall include the following opt-out icon to the right or left of 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 homepages. The icon shall be approximately the same size as any other icons used by the business on its webpage.

[Icon example]

Comments

Functional icons on webpages are typically larger than icons contained in the header or footer. Requiring header or footer icons to be the same size as general webpage icons may pose a readability issue for consumers (e.g., extending size of header or footer to accommodate the icon at the cost of information readability on the webpage). The Privacy Law Section also suggests that businesses be afforded flexibility to determine the design of the opt-out link in relation to other content on the webpage.

Proposed Alternative Language

§ 7015(b). A business that chooses to use an alternative opt-out link shall title the link "Your Privacy Choices" or "Your California Privacy Choices," and shall include the following opt-out icon ~~to the right or left of~~ 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 homepages. The icon shall be approximately the same size as any other icons used by the business in the header or footer of ~~on its~~ webpage.

ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

§ 7023. Requests to Correct.

Rule

§ 7023(b)(2). If the business is not the source of the personal information and has no documentation to support of (*sic*) the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.

Comments

The Privacy Law Section recommends removing subsection 7023(b)(2) in its entirety. It conflicts with the "totality-of-circumstances" approach incorporated into the draft regulations in subsection 7023(b)(1). Additionally, it is not consistent with the realities of the digital economy in which businesses purchase data sets from sophisticated third parties to achieve greater overall data accuracy. We ask the Agency to consider unintended consequences that may arise if individual consumer's assertions of inaccuracy are deemed to be the source of truth, especially when the business is not the source of the personal information.

Proposed Alternative Language

~~§ 7023(b)(2). If the business is not the source of the personal information and has no documentation to support of (sic) the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.~~

Rule

§ 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. 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.

(1) Business L maintains personal information about consumers that it receives from data brokers on a regular basis. Business L generally refreshes the personal information it maintains about consumers whenever it receives an update from a data broker. Business L receives a request to correct from a consumer and determines that the information is inaccurate. To comply with the consumer's request, Business L corrects the inaccurate information in its system and ensures that the corrected personal information is not overridden by inaccurate personal information subsequently received from the data broker. [...].

Comments

In response to a consumer request to correct, the business should correct the information that is inaccurate using "commercially reasonable efforts" as required in Civil Code section 1789.106(c). As such, we propose adding those terms to make the regulations consistent with the statute.

We also propose deleting example (1), particularly the suggestion that a consumer's correction should not be subsequently overridden by information a business may later receive from a data broker. Many sophisticated data brokers continuously update information about consumers, and it is therefore conceivable that the data a consumer initially "corrects" (e.g., that a consumer holds a professional license) will be later updated by the data broker to reflect subsequent developments (e.g., the consumer no longer holds the license). Requiring the business to treat the consumer's initial correction as the final word on the accuracy of that information could have the unintended consequence of preventing a business from incorporating into its database the most current information about the consumer, as provided by reliable third-party sources.

Proposed Alternative Language

§ 7023(c). A business that complies with a consumer's request to correct shall correct inaccurate the personal information using commercially reasonable efforts.~~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. 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.

[Delete Example (1)]

Rule

§ 7023(d)(2). A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following:

[...]

(C) The purpose for which the business collects, maintains, or uses the personal information. For example, if the personal information is essential to the functioning of the business, the business may require more documentation.

(D) The impact on the consumer. For example, if the personal information has a high impact on the consumer, the business may require less documentation.

Comments

Subsections 7023(d)(2)(C) and (D) address the amount of documentation a business “may require” in order to determine the validity of a consumer’s correction request. Subsection (C) authorizes businesses to require more documentation if the information subject to a correction request is essential to the functioning of the business, while subsection (D) indicates businesses may require less documentation if the information at issue has a “high impact on the consumer.”

We recommend deletion of the examples provided in subsections (C) and (D) because the quantity of documentation (e.g., more vs. less) that a business may request to rebut its determination that information is accurate may not be relevant to evaluating the veracity of the claimed inaccuracy. Rather, when conducting the holistic evaluation contemplated by this subsection, the guiding principle should be obtaining documentation that the business determines is necessary to ascertain the accuracy of the information at issue, including to prevent fraudulent attempts to change information. See Civ. Code § 1798.185(a)(8)(D). Whether “more” or “less” documentation is necessary for that determination will depend upon the nature of the documentation requested (e.g., governmental records vs. a personal attestation), not the importance to the business or the perceived impact on a consumer. Indeed, in some situations, when the information at issue will have a “high impact” on a consumer, a business may require the production of more, not less information (contrary to the proposed regulation) to ensure that the request to correct “high impact” data is not fraudulent.

Proposed Alternative Language

§ 7023(d)(2). A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following:

[...]

(C) The purpose for which the business collects, maintains, or uses the personal information. ~~For example, if the personal information is essential to the functioning of the business, the business may require more documentation.~~

(D) The impact on the consumer. ~~For example, the business may consider the types of documentation that are needed if a request to correct has a high impact on the consumer.~~

§ 7028. Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information.

Rule

§ 7028(c). If a consumer who has exercised their right to limit initiates a transaction or attempts to use a product or service that requires the use or disclosure of sensitive personal information for purposes other than those set forth in subsection (l), the business may inform the consumer that the transaction, product, or service requires the use or disclosure of sensitive personal information for additional purposes and provide instructions on how the consumer may provide consent to use or disclose their sensitive personal information for those additional purposes. The business shall comply with section 7004 when obtaining the consumer's consent.

Comments

The reference to subsection (l) is incomplete.

Proposed Alternative Language

If a consumer who has exercised their right to limit initiates a transaction or attempts to use a product or service that requires the use or disclosure of sensitive personal information for purposes other than those set forth in ~~subsection 7027(l)~~ ~~subsection (l)~~, the business may inform the consumer that the transaction, product, or service requires the use or disclosure of sensitive personal information for additional purposes and provide instructions on how the consumer may provide consent to use or disclose their sensitive personal information for those additional purposes. The business shall comply with section 7004 when obtaining the consumer's consent.

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

§ 7050. Service Providers and Contractors.

Rule

§ 7050(a). A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a “service provider” or “contractor” under the CCPA and these regulations, shall be deemed a service provider or contractor with regard to that person or organization for purposes of the CCPA and these regulations. For example, a cloud service provider that provides services to a non-profit organization and meets the requirements and obligations of a service provider under the CCPA and these regulations, i.e., has a valid service provider contract in place, etc., shall be considered a service provider even though it is providing services to a non-business.

Comments

In the CCPA, “Service Provider” is defined as “a person that processes personal information on behalf of a business and to that receives from or on behalf of the business a consumer’s personal information for a business purpose pursuant to a written contract....” Therefore, it is clear that an entity becomes a Service Provider only when it is processing information on behalf of a business (as defined in the CCPA). Instead of saying service providers for non-profit entities are in scope for CCPA as service providers, the regulations should clarify that service providers for non-profits are not in scope for CCPA.

Proposed Alternative Language

§ 7050(a). A business that provides services to a person or organization that is not a business is not a “service provider” or “contractor” under the CCPA and these regulations. ~~and that would otherwise meet the requirements and obligations of a “service provider” or “contractor” under the CCPA and these regulations, shall be deemed a service provider or contractor with regard to that person or organization for purposes of the CCPA and these regulations.~~ For example, a cloud service provider that provides services to a non-profit organization and meets the requirements and obligations of a service provider under the CCPA and these regulations, i.e., has a valid service provider contract in place, etc., shall not be considered a service provider under the CCPA to the extent even though it is providing services to a non-business.

Rule

§ 7050(b). A service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except:

[. . .]

(5) To detect data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity.

Comments

The proposed regulations provide six examples of the types of processing a service provider or contractor may undertake. We propose adding “or to investigate” to allow service providers to not only detect but also to investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity.

Proposed Alternative Language

§ 7050(b). A service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except:

[. . .]

(5) To detect or to investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity.

§ 7051. Contract Requirements for Service Providers and Contractors.

Rule

§ 7051(a). The contract required by the CCPA for service providers and contractors shall:

[...]

(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).

(4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any commercial purpose other than the business purposes specified in the contract, including in the servicing of a different business, unless expressly permitted by the CCPA or these regulations.

Comments

Section 7051(a) provides ten requirements for a service provider or contractor contract. It is unclear whether the Agency is proposing that all ten requirements must be separate clauses in the contract. As stated in the ISOR, “Subsections (a)(3) and (4) are derived from the same Civil Code section, but they have been broken up into two separate requirements to make it easier for businesses to read and understand.” We propose deleting subsection 7051(a)(4) and revising subsection 7051(a)(3) to clearly and closely follow what the statute says in Civil Code section 1798.140 (j)(1)(A)(ii) and (ag)(1)(B).

Proposed Alternative Language

§ 7051(a). The contract required by the CCPA for service providers and contractors shall:

[...]

(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 for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose. ~~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).

~~(4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any commercial purpose other than the business purposes specified in the contract, including in the servicing of a different business, unless expressly permitted by the CCPA or these regulations.~~

Rule

§ 7051(a). The contract required by the CCPA for service providers and contractors shall:

[...]

(5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information received from, or on behalf of, the business with personal information that it received from another source unless expressly permitted by the CCPA or these regulations.

Comments

Civil Code section 1798.140(ag)(1)(D) allows service providers or contractors to combine personal information to perform any business purpose, which may include providing advertising and marketing services. However, under Civil Code section 1798.140(e)(6), a service provider or contractor may not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another business or collects from its own interaction with consumers. Our proposed revisions make it clear that providing advertising and marketing services can be part of the service that a service provider or contractor provides to the business, but that the advertising and marketing services should only be provided with the restrictions under Civil Code section 1798.140(e)(6), which prohibit certain types of personal information from being combined with other types of personal information as specified in the statute.

Proposed Alternative Language

§ 7051(a). The contract required by the CCPA for service providers and contractors shall:

[...]

(5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider may provide advertising and marketing services to the business, but the service provider may not combine the personal information of a consumer who has directed the business to opt them out of sales or sharing with personal information that the service provider receives from another business or collects from its own interaction with consumers. ~~or contractor shall be prohibited from combining or updating personal information received from, or on behalf of, the business with personal information that it received from another source unless expressly permitted by the CCPA or these regulations.~~

Rule

§ 7051(a). The contract required by the CCPA for service providers and contractors shall:

[...]

(8) Require the service provider or contractor to notify the business no later than five business days after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

Comments

Section 7051(a)(8) is one of ten requirements proposed by the Agency as contract requirements for service providers and contractors. As stated in the ISOR, the Agency may believe and it may be true that five business days is the reasonable amount of time for the service provider or contractor to notify the business that it has made a determination it can no longer meet its obligations under the CCPA and these regulations. However, we do not believe the Agency is proposing that a written contract with a service provider or contractor would be deemed to be non-compliant and therefore the entire relationship would no longer be deemed to be a service provider or contractor relationship under the CCPA if the contract does not have this exact language in the contract. Because this list of requirements is understood to be requirements for a contract between the business and all its service providers and contractors, including a specific number of days in the requirement may result in the unintended consequence of requiring businesses to renegotiate and amend even the contracts that meet the spirit of the law. We recommend removing a reference to a specific number of days and replacing it with “promptly.”

Proposed Alternative Language

§ 7051(a). The contract required by the CCPA for service providers and contractors shall:

[...]

(8) Require the service provider or contractor to notify the business ~~promptly no later than five business days~~ after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

Rule

§ 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.

Comments

The ISOR states “Businesses, service providers, and contractors are to comply with not just the letter of the law, but the spirit of the law.” Applying the same, we ask the Agency to clarify that the Agency does not intend for the ten requirements as proposed in subsection 7051(a) to be ten separate clauses in a written contract word for word. Instead, we propose revisions in subsection 7051(c) to allow for businesses, service providers, and contractors to enter into contracts that meet the spirit of the requirements under the CCPA to be deemed a service provider or a contractor under CCPA.

The proposed revisions also remove the double negative.

Proposed Alternative Language § 7051(c). A person who has ~~does not have~~ a contract that reasonably complies with each of the subsections under subsection (a) ~~is~~ may be deemed not to be 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.

* * *

Respectfully submitted,

Privacy Law Section of the California Lawyers Association

From: **Cher Gonzalez** [REDACTED]
To: **Regulations** <Regulations@cpga.ca.gov>
Cher Gonzalez [REDACTED]; **David Gonzalez**
CC: [REDACTED]; **JD Cher Gonzalez**
Subject: CPPA Proposed Regulations: Comments
Date: 23.08.2022 23:27:42 (+02:00)
Attachments: CLSFinalCopyCommentsPrivacyProposedRegs8.22.pdf (3 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear CPPA,

On behalf of our client, California Life Sciences, ("CLS") we thank you for the opportunity to submit the attached comments during the public comment period regarding proposed regulations to amend the current California Consumer Privacy Act Regulations, which are necessary to implement the California Privacy Rights Act of 2020.

Cher Gonzalez, Esq.

Partner

RESOLUTE

and

Gonzalez Government Consulting

Mobile: [REDACTED]

Emails [REDACTED]
[REDACTED]

1215 K Street, Suite 1100
Sacramento, CA 95814

www.ResoluteCompany.com



August 23, 2022

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

Submitted electronically to: regulations@coppa.ca.gov

Re: California Consumer Privacy Act Proposed Regulations: Public Comment Period, as Noticed on July 8, 2022

Dear California Privacy Protection Agency:

On behalf of California Life Sciences, (Hereinafter “CLS”) I thank you for the opportunity to submit comments during the public comment period regarding proposed regulations (Hereinafter “proposed regulations”) to amend the current California Consumer Privacy Act Regulations, which are necessary to implement the California Privacy Rights Act of 2020 (Hereinafter “underlying statute”) approved by California voters via the initiative process.¹ CLS is a premiere statewide advocacy organization working with industry, government, academia, and others to shape public policy, improve access to innovative technologies. For more than 30 years, CLS has served the community by supporting companies of all sizes, from early-stage innovators and startups to established industry leaders in the fields of biotechnology, pharmaceuticals, and medical technology. As integral components of a healthy and collaborative ecosystem, CLS also works closely with universities, academic and research institutions, and other critical partners that promote this vibrant sector. CLS is concerned that the current draft of the proposed regulations could have a detrimental impact on our members, particularly our small start-up members focused on discovering new medical breakthroughs, which often have few employees and limited funding. As a result, we have three recommendations for changes to the proposed regulations, which are explained below.

1. **CLS Requests the Term “Detailed Explanation” in Section 7022(f)(1) be Defined, or in the Alternative, Examples of a “Detailed Explanation” be Included Within the Final Regulations.**

¹ California Privacy Rights Act, California Civil Code Sections 1798.100 - 1798.199.100, Amended November 3, 2020, by initiative Proposition 24, Sec. 13. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.



Subsection (f)(1) of Section 7022 of the proposed regulations requires businesses that deny a consumer “request to delete” to provide to the consumer a “detailed explanation” of the basis for the denial. However, “detailed explanation” is not defined within the regulation, yet “request to delete” is defined in Section 7001(v). As a result, CLS urges amending the definitions section of the proposed regulations (Section 7001) to clearly define “detailed explanation” or provide an example within the final regulations, to aid our membership in complying with the requirements in Section 7022(f)(1).

2. CLS Requests Section 7051(e) be Stricken as it Exceeds Statutory Authority and is Overly Burdensome.

Subsection (e) of Section §7051 of the proposed regulations states that a business which “never enforces the terms of the contract nor exercises its rights to audit or test” a service provider’s systems “might not be able to rely on the defense it did not know and should not have known of a service provider’s violation.” Civil Code Section 1798.100(d)(3) of the underlying statute requires businesses that share consumer personal information with third parties to have contracts that grant the business rights to “take reasonable and appropriate steps” to help ensure that the third party uses the personal information consistent with the business’ obligations. Further, Section 1798.135(g) of the underlying statute states that a business shall not be liable for a third-party violation of a consumer’s opt-out request if the business did not “have actual knowledge, or reason to believe” that the third party intends to commit such a violation. CLS contends that inferring that conducting audits or tests are necessary to establish that a business did not have “reason to believe” goes beyond the requirements of businesses as contained in the underlying statute. Finally, Civil Code Section 1798.185(a)(7) states that the “burden on the business” should be taken into account when establishing rules in furtherance of Sections 1798.105, 1798.106, 1798.110 and 1798.115. CLS contends that the inference in Section 7051(e) of the proposed regulations that audits or tests would be necessary for a business to establish “due diligence” does not take into account the burden on our life science members, particularly small start-ups engaged in research, which may not have the headcount capacity or funding to engage in regular audits, but which still engage in steps that are “reasonable and appropriate” to ensure that a third party use of the information is consistent with the statute. As a result, we ask that Section 7051(e) be stricken.

3. CLS Requests that Section 7025(e) be Stricken as it is Contrary to the Underlying Statute.

Subsection (e) of Section 7025 of the proposed regulations states that Section 1798.135(b)(1) and (3) of the underlying statute provides a business a choice between processing opt-out preference signals by providing opt-out links, or processing opt-out



preference signals in a “frictionless manner” which is defined. Subsection (e) goes further to state that Section 1798.135(b)(1) and (3) “does not give the business a choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preferences signals, though it may do so in a frictionless manner.” However, this is in contradiction to the underlying statute, specifically Civil Code Section 1798.135. Subsection (a) of Section 1798.135 states that a business shall provide a “clear and conspicuous link” to opt-out, while subsection (b) states that a business is not required to comply with subdivision (a) if the business allows consumers to opt out through the use of an opt-out preference signal. Further, subsection (b)(3) of the underlying statute goes on to state:

“(3) A business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).”

As a result, CLS requests Section 7025(e) be stricken from the proposed regulations since it is in direct conflict with the underlying statute.

CONCLUSION

CLS’s public policy work is focused on fulfilling its mission to nurture California’s life sciences industry, empowering medical discoveries that lead to healthier lives for people around the world. CLS is concerned that the above referenced sections of the proposed regulations would, if not amended, have a detrimental impact on California’s vibrant life science community engaged in research and development in the fields of biotechnology, pharmaceuticals, and medical device technology. Thank you for your consideration of our suggested changes to the current draft proposed regulations. Should you wish to discuss these items you may reach me at

Sincerely,

Sam Chung
Vice President, State Government Relations
California Life Sciences

From: **Lisa Quaranta** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment - California Credit Union League Comment Letter
Date: 23.08.2022 23:28:50 (+02:00)
Attachments: CPPA - Ltr RE CCPA Proposed Regs - 082222.pdf (10 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello:

Attached please find the California Credit Union League's comment letter re: CPPA Public Comment – Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA).

We appreciate the opportunity to comment on this matter and for considering our views.

Thank you,

Lisa Quaranta

Vice President, Regulatory Advocacy & Compliance
California & Nevada Credit Union Leagues

D: [REDACTED] | www.ccul.org



We Are Committed To Helping Credit Unions Change People's Lives

The information contained in this email message and any attachments to this message are intended only for the person or entity to which it is addressed, and may be proprietary, confidential, and/or privileged. If you are not the intended recipient, please: (1) notify the sender immediately by replying to this message; (2) do not use, disseminate, distribute, or reproduce any part of the message or any attachment; and (3) destroy all copies of this message and attachments. Please let us know if you have any questions.



August 22, 2022

California Privacy Protection Agency
 Attn: Brian Soublet
 2101 Arena Boulevard
 Sacramento, CA 95834
 Via Email: (regulations@coppa.ca.gov)

Re: **CCPA Public Comment**

Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

Dear Mr. Soublet:

I am writing on behalf of the California Credit Union League (League), one of the largest state trade associations for credit unions in the United States, representing the interests of approximately 230 California credit unions and their more than 11.6 million members.

On July 8, 2022, the California Privacy Protection Agency (CPPA) began its formal rulemaking activities in connection with the administration and enforcement of the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA) (collectively, CCPA/CPRA).

The League has significant concerns with a number of aspects of the CCPA/CPRA and the proposed regulations, including: (1) several areas in the proposed regulations that appear to exceed the requirements of CCPA/CPRA; (2) the potential audits to be performed by the CPPA; (3) the effective date; (4) the enforcement date; (5) a lack of clarity around the exemption for personal information collected pursuant to the federal Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (CFIPA); and (6) the lack of model notices to facilitate compliance.

We respectfully offer the following comments.

1. Proposed Regulations Exceed Statute Requirements

Many areas in the proposed regulations appear to exceed the requirements of the statute—requiring more detailed levels of explanation to the consumer, written confirmations beyond what the statute indicated, and additional steps. While the CPPA was given broad statutory authority to establish rules and procedures to implement and further the purposes of the CCPA/CPRA, some of these additional proposed requirements create an unnecessary burden on businesses and should be reconsidered.

The following outlines our specific concerns:

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

Under Calif. Civil Code §1798.100, businesses need to provide notice to consumers at the point of collection regarding the categories of personal information collected and the purposes for which the information will be used. Before a business collects additional categories of personal information or uses personal information for additional purposes that are incompatible with the disclosed purposes, a consumer must receive a supplementary notice.

Section 7002(a) of the proposed regulations would require a business to obtain the consumer’s “explicit consent” 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.

This exceeds the statutory requirement and creates a new “opt-in” requirement. We recommend replacing this requirement with a new notice to the consumer along with a 30-day opportunity to opt-out, which is more consistent with the statutory intent.

B. §7023. Requests to Correct

The CPRA has amended the CCPA to add a new right: the Right to Request Correction of Inaccurate Personal Information (Calif. Civil Code §§1798.106 and 1798.130).

Section 7023(f) adds additional layers of notice requirements when a consumer submits a request to correct inaccurate information. Not only must the business provide specific notices and explanations to the consumer with regard to its response, §7023(f)(3) of the proposed regulations now requires businesses that receive a consumer request to correct inaccurate information to also inform any person with whom it discloses, shares, or sells the personal information that the consumer contests the accuracy of the information, adding yet another notice requirement on the business not established under the statute. Moreover, it does not afford the business a reasonable opportunity to investigate the validity of the claim or the accuracy of the information before it is under an obligation to notify third parties.

In addition, §7023(i) of the proposed regulations requires businesses, when they are not the source of the inaccurate information, to provide consumers with the name of the source from which the businesses receive the alleged inaccurate information. This exceeds the original statute and may create significant compliance and technological challenges for a credit union without a data inventory or data mapping program.

C. §7024. Request to Know

Under Calif. Civil Code §1798.130(a)(2)(B), a business is required to respond to a request to know with specific pieces of personal information that the business has collected about the consumer for the 12-month period preceding the business’s receipt of the request and beyond pursuant to a regulation.

Under the proposed regulations, §7024, a business **must provide** the consumer “[a]ll the personal information it has collected and maintains about the consumer on or after January 1, 2022, including beyond the 12-month period preceding the business’s receipt of the request, unless doing so proves impossible or would involve disproportionate effort.”

This requirement proposed in the regulation contradicts the current requirement under the statute, which states that a business is only required to provide personal information from the prior 12 months **unless the consumer requests** that the business provide information beyond the 12-month period. We believe that the regulation’s more expansive requirement is problematic and would create an additional burden on businesses.

D. §7025. Opt-Out Preference Signal

Calif. Civil Code §1798.135(b) provides that a business that sells or shares consumers’ personal information or uses or discloses consumers’ sensitive personal information for purposes other than as expressly authorized shall not be required to provide opt-out links on its website *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.

However, under §7025 of the proposed regulations, a business that sells or shares personal information would *always* be required to process a consumer’s request via an opt-out preference signal, although if it posts the opt-out links, it may process opt-out preference signals in a non-frictionless manner.

Because the CCPA/CPRA has been interpreted to give businesses the *option* to process and comply with opt-out preference signals instead of implementing Opt-Out Links or Alternative Opt-Out Links, we believe that the proposed regulations contradict this interpretation and may create significant compliance and technological challenges, especially for our smaller credit unions.

E. §7027. Requests to Limit Use and Disclosure of Sensitive Personal Information

Calif. Civil Code §1798.121 gives consumers the right to request a business to limit its use and/or disclosure of their sensitive personal information.

The proposed regulations, at §7027(l), set forth a list of purposes for which a business may use or disclose sensitive personal information without offering the right to limit the use or disclosure of such information (e.g., to perform the goods or services requested, to detect security incidents, to prevent fraud, etc.). However, the proposed regulations do not clarify when sensitive personal information is to be considered “collected” or “processed” when the business is inferring characteristics about the affected consumer. We believe the lack of clarity in this area could potentially create confusion and possible unintended violations of CCPA/CPRA.

F. §7050. Service Providers and Contractors

Section 7050 of the proposed regulations cites the following example to help clarify when a business that provides services to a person or organization that is not a business, as defined, might be deemed a “service provider” or a “contractor”:

“[A] cloud service provider that provides services to a non-profit organization and meets the requirements and obligations of a service provider under the CCPA and these regulations, i.e., has a valid service provider contract in place, etc., shall be considered a service provider even though it is providing services to a non-business.”

The example stated above is confusing. Is it the CCPA’s position that services rendered to a non-profit entity would be subject to the CCPA/CPRA requirements even though CCPA/CPRA exempts non-profits from its application? We respectfully ask that the final regulations clarify whether the exemption applies to or excludes non-profit entities.

2. Burden of Potential Agency Audits to Highly Regulated Businesses

Calif. Civil Code §1798.199.65 gives the CCPA the authority to audit businesses’ compliance with the law. The proposed regulations (§7304) would allow the CCPA to perform audits in three situations: (1) to investigate possible violations of the CCPA/CPRA; (2) if the subject’s collections or processing activities present significant risk to consumer privacy or security; or (3) if the subject has a history of noncompliance with the CCPA/CPRA or any other privacy protection laws. Moreover, these audits maybe announced or unannounced, and a business’s failure to cooperate with an audit could lead to enforcement action against that business.

Pending further clarification regarding the definition of a “business” as discussed in Section 7 below, credit unions may be subject to the CCPA/CPRA and therefore to audits performed by the CCPA. Moreover, the CCPA’s enforcement authority could extend to both state and federally chartered credit unions.

As financial institutions, credit unions are already among one of the most highly regulated industries. California’s state-chartered credit unions are licensed and regulated by the California

Department of Financial Protection and Innovation (DFPI), and the National Credit Union Administration (NCUA) regulates federal credit unions as well as federally insured state credit unions. Additionally, credit unions are subject to federal Consumer Financial Protection Bureau (CFPB) oversight, among other agencies. Credit unions currently undergo robust examinations by their regulatory agencies, which includes their compliance with applicable state and federal privacy and data security laws and regulations. We are concerned that potential audits conducted by CCPA would be not only duplicative of existing examination requirements, but unjustifiably intrusive, burdensome, and overreaching for credit unions. The burden of these additional audits on smaller financial institutions could be especially significant in terms of disruption to staffing and operations. Therefore, we believe that a clear exemption is warranted.

However, if the CCPA is unwilling to provide such an exemption for credit unions, then it must provide guidance as to how credit unions can comply without unnecessarily burdening the credit union industry. At a minimum, coordination with state and federal primary regulators would be warranted.

3. Effective Date

The CCPA/CPRA is effective January 1, 2023. However, the proposed regulations were not issued until July 8, 2022, and they expanded the compliance obligations over that of the current CCPA in a number of areas. Given the detailed and technical nature of the proposed regulations, as well as the extensive technical and operational steps that will be required to ensure full compliance, it is only fitting that the CCPA/CPRA effective date should be extended.

Covered businesses need adequate time to understand the requirements of the statute and the final regulations prior to designing and implementing comprehensive compliance solutions appropriate to the size and scope of their operations, as well as the time and financial resources to actually design and implement those solutions and adequately train staff. The Leagues recommend that the CCPA delay the effective date by two years, until January 1, 2025.

4. Enforcement Date

The CCPA/CPRA provides that the CCPA can bring enforcement action six months after publication of the final regulations or July 1, 2023, whichever is sooner. That means the CCPA could literally adopt final regulations on June 30, 2023, and enforce the law and the regulations the next day, on July 1, 2023.

While we understand that this is not the most likely scenario, it is still a serious concern. As stated above, covered businesses should have adequate time to understand the requirements of the statute and the final regulations, and sufficient time to design and implement comprehensive compliance solutions before being subjected to enforcement actions. Due to the complexities of the

CCPA Public Comment – Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)
August 22, 2022
Page 2

CCPA/CPRA, we urge the CCPA to delay enforcement until no less than six months after publication of final regulations.

5. GLBA and CFIPA Exemptions

The CPRA revised the CCPA’s financial information exception to apply to “personal information collected, processed, sold, or disclosed *subject* to the federal Gramm-Leach-Bliley Act . . . , or the California Financial Information Privacy Act...” (emphasis and revision added).

Regardless of this change, there is still significant confusion regarding the exemption for personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (CFIPA). The confusion arises because the CCPA/CPRA uses terms that are inconsistent with the GLBA and CFIPA.

- The GLBA and CFIPA both use the terms “nonpublic personal information” and define that term to mean “personally identifiable financial information.”
- The CCPA/CPRA uses the term “personal information,” which is defined in Calif. Civil Code §1798.140(o) and is much broader than the GLBA/CFIPA’s definition of “nonpublic personal information.”
- In addition, the GLBA pertains to “personally identifiable financial information” collected in the course of a transaction or providing a financial product or service, etc. The CCPA/CPRA pertains to personal information collected in basically any manner, including when there is no transaction.

Because of the inconsistent terminology, the exemption provided in Calif. Civil Code §1798.145(e) is unclear and can be interpreted several ways. It is essential that the CCPA provide clarification in the regulations.

Moreover, for financial institutions that are only subject to the CCPA/CPRA notice requirements to the extent not covered by an exemption, guidance with regard to the appropriate response to a consumer that recognizes this exemption would be especially useful, given that consumers are unlikely to be familiar with the nature and extent to which the exemption applies.

6. Model Notices Needed

The CCPA and its regulations created several notice requirements for businesses, including:

- Notice at or Before Collection,
- Right to Opt-Out,
- Notice of Financial Incentives, and
- Updated Privacy Notices.

CPPA Public Comment – Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)
August 22, 2022
Page 2

Further, the regulations require specific responses to certain verifiable consumer requests, for which model forms for both the request and the response would be beneficial:

- Verifiable Consumer Request to Know,
- Response to Verifiable Consumer Request to Know,
- Verifiable Consumer Request to Delete,
- Response to Verifiable Consumer Request to Delete,
- Verifiable Consumer Request to Limit the Use of Sensitive Personal Information, and
- Response to Verifiable Consumer Request to Limit the Use of Sensitive Personal Information.

As noted above, the CPRA added the new Right to Request Correction of Inaccurate Personal Information, which would require a specific response to another form of verifiable consumer request. Useful Model forms would include:

- Verifiable Consumer Request to Correct Inaccurate Personal Information, and
- Response to Verifiable Consumer Request to Correct Inaccurate Personal Information.

Additionally, businesses must provide notice of the following consumer requests to third party service providers and contractors:

- Notice to Third Party Service Provider/Contractor that Consumer Contests the Accuracy of Certain Personal Information,
- Notice to Third Party Service Provider/Contractor of Consumer Opt-Out Request,
- Notice to Third Party Service Provider/Contractor of Consumer Deletion Request, and
- Notice to Third Party Service Provider/Contractor of Consumer Request to Limit the Use of Sensitive Personal Information.

For all these required notices and responses, the regulations require the notices be easy to read and understandable by the average consumer and provide some standards to achieve that. This direction is subjective and does not contemplate a method or metric to assess the readability.

Since all businesses need to provide the required notices and responses, uniform model notices would help ensure consumer's understanding of the notices, simplify the requirements for businesses, and create an objective standard of review to determine whether a business' notices comply with the required standards. The Leagues recommend the CPPA draft proposed model notices for public comment and then include a safe harbor in the final regulations for the use of notices substantially similar to the model notices.

The provision of model notices by the CPPA will also help to alleviate some of the initial compliance burden associated with meeting the fast-approaching Effective Date and Enforcement Date.

7. Other Considerations

A. The Credit Union Difference

The League supports the spirit of the law; however, it is important that the CPPA understand the credit union difference. Credit unions, while highly regulated financial institutions, are first and foremost member-owned, democratically governed, not-for-profit financial cooperatives whose purpose is to promote thrift and improve access to credit for their member-owners, particularly those of modest means. As not-for-profit entities, credit union earnings are passed on to their member-owners in the forms of reduced fees, higher savings rates, and lower loan rates. Credit unions exist for the financial benefit of their member-owners, but they are ultimately driven by the philosophy of people-helping-people.

The credit union structure is vastly different than for-profit entities. “Owners” are not proprietors or shareholders in a business whose only goal is that the business maximize individual shareholder profits. Instead, credit union shareholders are members of a not-for-profit cooperative with a volunteer board of directors democratically elected by and from among its members. Each member has one vote, regardless of the number of shares (amount of funds) held in the credit union. Consumer personal information collected by credit unions is the personal information of its member-owner consumers in order to provide them with the products and services they desire.

Credit unions are the original consumer financial protection advocates. In addition, as highly regulated insured depository institutions, credit unions already comply with a plethora of data privacy and security requirements, including GLBA, CFIPA, and NCUA’s data security regulations.

B. Definition of a Business

The definition of a “business” subject to the requirements of the CCPA/CPRA requires further clarification.

- Thresholds

The CPRA changed the scope of covered businesses. Part of the definition of a business is that it satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys or sells, or shares the personal information of 100,000 or more consumers or households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal Information.

The application of threshold (B) to the personal information of 100,000 or more “consumers or households” is confusing. A consumer, as defined in the CCPA/CPRA is a natural person California resident. Is the rest of the threshold then related to households of natural person California residents? Additionally, further clarification is needed to determine the method for counting the number of consumers or households toward the 100,000 threshold. For example, if one household has five individual residents/consumers, would they be counted as one (household), five (consumers) or six (five consumers plus one household) toward the 100,000 threshold? For smaller credit unions, these distinctions are essential to the determination of whether they are subject to the requirements of the CCPA/CPRA.

- *Doing Business in California*

Another part of the definition of a business is that the entity “does business in the State of California.” There is no clear definition under the CCPA/CPRA or the regulations of what it means to “do business” in the State of California. Clarification is needed.

For credit unions based outside of California, members may live in or relocate to California while maintaining a relationship with their out of state credit union through ATMs or a shared branching network. (A shared branching network allows a member of one credit union to walk into the local branch of another credit union of which they are not a member and perform a range of transactions.)

At what point does the non-California credit union become subject to the CCPA/CPRA despite the lack of a physical presence? “Doing business” in a state should mean something more than isolated or incidental transactions. There should be a clearly defined standard that contemplates intentional repeated and successive transactions that clearly indicates a pattern or practice of choosing to do business with California consumers, and not one-time or occasional transactions.

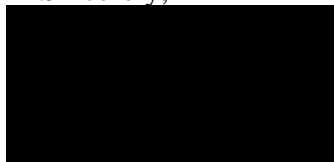
CPPA Public Comment – Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)
August 22, 2022
Page 2

Final Comments

Ultimately, the League supports the spirit of the law and the need to protect the personal information of its members, but we continue to have significant concerns with the practicality and implementation of the proposed regulations.

We thank you for the opportunity to comment. We trust you will carefully consider our views and recommendations. If you have any questions regarding our comments, please contact me.

Sincerely,



Diana R. Dykstra
President/CEO
California Credit Union League

From: **Shapiro, Tracy** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Holman, Eddie** [REDACTED]
Subject: CPPA Public Comment
Date: 23.08.2022 23:39:24 (+02:00)
Attachments: 2022-08-23 CPPA Public Comment (Wilson Sonsini).pdf (9 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Board Members and Staff of the California Privacy Protection Agency:

Please find attached our comments in response to the California Privacy Protection Agency's invitation for comments on its proposed rulemaking under the California Privacy Rights Act of 2020, Cal. Code Regs. tit. 11, §§ 7000-7304. We submit these comments with the aim of encouraging the Agency to issue regulations that will protect the privacy of consumers in a manner that is effective, practical, and allows companies to continue to provide consumers with valuable services.

Thank you,
Tracy Shapiro



Tracy R. Shapiro | Partner, Privacy & Cybersecurity | Wilson Sonsini Goodrich & Rosati
One Market Street | San Francisco, CA 94105 | O: [REDACTED] | [REDACTED]

This
email
and

any attachments thereto may contain private, confidential, and privileged material for the sole use of the intended recipient. Any review, copying, or distribution of this email (or any attachments thereto) by others is strictly prohibited. If you are not the intended recipient, please contact the sender immediately and permanently delete the original and any copies of this email and any attachments thereto.



Wilson Sonsini Goodrich & Rosati
Professional Corporation
One Market Plaza
Spear Tower, Suite 3300
San Francisco, California 94105-1126
O: 415.947.2000
F: 415.947.2099

August 23, 2022

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

Re: CPPA Public Comment

Dear Board Members and Staff of the California Privacy Protection Agency:

Wilson Sonsini Goodrich & Rosati appreciates the opportunity to submit these comments in response to the California Privacy Protection Agency's ("CPPA" or "Agency") invitation for comments on its proposed rulemaking under the California Privacy Rights Act of 2020 ("CPRA"), Cal. Code Regs. tit. 11, §§ 7000-7304 ("Proposed Regulations"). We submit these comments on behalf of certain of our clients, including companies that provide connected devices, such as over the top ("OTT") devices. To be clear, these comments do not necessarily reflect the views of all of our clients. These companies appreciate the importance of consumer privacy and data protection, and we submit these comments with the aim of encouraging the Agency to issue regulations that will protect the privacy of consumers in a manner that is effective, practical, and allows companies to continue to provide consumers with valuable services.

1. Section 7013(e)(3)(C) of the Proposed Regulations is redundant and not required by the CPRA, and should therefore be removed.

Section 7013(e)(3)(C) of the Proposed Regulations requires that a business that sells or shares personal information that it collects through a connected device (*e.g.*, a smart television or smart watch) provide a notice of right to opt out of sale/sharing in a manner that ensures that the consumer will encounter the opt-out notice while using their device. The requirement to provide an opt-out notice while the consumer is "using the device" is not required by the CPRA. Rather, Section 1798.135(a) of the CPRA requires that businesses provide a link to the opt-out notice from the business's homepage. Moreover, because Section 7012(e)(5) of the Proposed Regulations already requires businesses to provide a link to the opt-out notice in their notice at collection, this separate opt-out notice requirement is redundant and should be removed.

In the alternative and at a minimum, if the Agency does not remove the requirement of Section 7013(e)(3)(C) from the Proposed Regulations, the Agency should clarify that businesses

California Privacy Protection Agency
Mr. Brian Soublet
Page 2

are not required to provide the opt-out notice *on the actual device*, so long as the consumer receives the opt-out notice through another means, for example on a website where the consumer registers the device. In many instances it will be impractical, if not impossible, for connected devices to provide legal notices through the device, such as when configuring an Internet-connected washing machine or light switch, or any other connected device with a limited external interface, such as a smart watch. Even for connected devices that could theoretically display a legal notice, such as a connected TV, the firmware on these devices frequently cannot be updated on the same time frame as a website. Firmware for these devices is frequently updated only on a set annual or biannual cycle due to the difficulties inherent in deploying code updates to a wide range of devices that are in active use by millions of households. It may take 6-12 months for a firmware update to be developed, coded, tested, and translated, and several more months for the update to be fully deployed, and doing so may consume substantially more engineering resources than coding an equivalent change to the organization's webpage would require. In light of the rapid clip at which new US state privacy laws and regulations are being enacted, it is not realistic for OTT providers to continually update their firmware each time a new disclosure requirement takes effect.

Therefore, if the Agency chooses to include a requirement that businesses provide an opt-out notice and ensure that consumers see it (despite a lack of authority to do so), connected devices should be able to meet that requirement by providing the notice in an alternative manner (for example, on the business's homepage, if visiting the business's website or app is a necessary step to activate the device). Moreover, the Agency seems to be applying this requirement to ensure that the consumer *will encounter* the opt-out notice of some businesses (e.g., providers of connected devices and virtual or augmented reality services) but not of others (e.g., apps and websites that only have to post a link to the notice).

2. The Proposed Regulations should not require businesses to honor opt-out preference signals.

The Proposed Regulations' requirements under Section 7025(b) that businesses "shall process any opt-out preference signal . . . as a valid request to opt-out of sale/sharing" and Section 7026(a)(1) that businesses "shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal" are inconsistent with the requirements for an opt-out preference signal under Section 1798.185(a)(19)-(20) of the CPRA. In particular, the requirements under the Proposed Regulations do not make honoring the signal optional, as is required by Section 1798.135(b)(3) of the CPRA.

The CPRA is explicit that honoring opt-out preference signals is optional. Section 1798.135(b)(3) of the CPRA specifically states that a business that offers "Do Not Sell or Share My Personal Information" or "Limit the Use of My Sensitive Personal Information" links on their

California Privacy Protection Agency
Mr. Brian Soublet
Page 3

homepage is not required to honor opt-out preference signals. Lest there be any confusion on the issue, the CPRA clarifies that, “For the purposes of clarity, a business may elect whether to comply with [the subdivision requiring opt-out links] or [the subdivision allowing consumers to opt out via opt-out preference signals].”

The Agency attempts to refute this interpretation of Sections 1798.135(b)(1) and (3) in Section 7025(e) of the Proposed Regulations. Specifically, the Agency states that, rather than giving businesses a choice between honoring opt-out preference signals or providing opt-out links, those CPRA subdivisions give businesses a choice between providing opt-out links or processing opt-out preference signals in a “frictionless manner,” a newly-created term in the Proposed Regulations that has no equivalent in the CPRA. The Agency’s Initial Statement of Reasons (“ISOR”) to the Proposed Regulations further states that “[t]o the extent that businesses are confused by the language in Civil Code section 1798.135, subdivision (e), which references subdivision (b)(1), of these regulations make clear that businesses must comply with an opt-out preference signal regardless of whether or not they post the identified opt-out links.” Contrary to the Agency’s claim, however, Section 7025(e) of the Proposed Regulations does nothing to clarify the language in Section 1798.135(e) of the CPRA, but rather attempts to change the plain meaning of that language. Section 1798.135(e) is consistent with Section 1798.135(a)-(b), and reinforces that businesses may choose whether to comply with subdivision (a) or (b). Section 1798.135(e) merely adds that consumers may authorize another person to opt out of the sale or sharing of the consumer’s personal information on the consumer’s behalf, and that businesses must honor those opt-out requests. This would include honoring an opt-out preference signal sent by a person authorized by the consumer, where the business chose to honor such signals in place of implementing opt-out links.

To the extent that the Agency is asserting that Section 1798.135(e) of the CPRA requires businesses to treat an opt-out preference signal as a “person” authorized by the consumer to exercise an opt-out right on the consumer’s behalf (as some have argued in other comments), that assertion fails because it ignores the definition of “person” under Section 1798.140(u) of the CPRA, i.e., “an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.” A “signal” is plainly none of these things. Because of this fundamental inconsistency and to avoid the unnecessary expenditure of resources by businesses to comply with a regulatory requirement that conflicts with the text of the statute, the Agency should revise Sections 7025 and 7026 of the Proposed Regulations to make clear that, consistent with the CPRA statute, honoring opt-out preference signals is optional.

3. Section 7025 of the Proposed Regulations fails to provide any meaningful or actionable technical specifications for an opt-out preference signal.

California Privacy Protection Agency
Mr. Brian Soublet
Page 4

Section 1798.185(a)(19)(A) of the CPRA mandates that the Attorney General issue regulations “defin[ing] the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism.” The Proposed Regulations, however, fail to provide any meaningful technical specifications that would allow businesses to know what opt-out preference signals to look for. Because the Proposed Regulations fail to provide meaningful technical specifications for an opt-out preference signal, Section 7025 of the Proposed Regulations should be struck in its entirety until such specifications are developed.

As explained in more detail below, the Proposed Regulations provide only two criteria that purport to be “technical specifications,” and neither provides sufficient parameters for businesses to understand how to recognize such signals and implement compliant technical solutions.

- (i) *The Proposed Regulations’ requirement that the signal “be in a format commonly used and recognized by businesses” is overly broad and provides no meaningful guidance to businesses.*

Section 7025(b)(1) of the Proposed Regulations provides that a valid opt-out preference signal “shall be in a format commonly used and recognized by businesses” and provides, as its only example “an HTTP header field.” Even if the Agency did have authority to require businesses to honor opt-out preference signals, for at least three reasons Section 7025(b)(1) of the Proposed Regulations is unworkable and vague, and should be struck until it is replaced with more specific guidance.

First, the *format* of a signal is only one factor in defining the specifications of a signal. The Proposed Regulations fail to provide any other factors that would put a business on notice that a particular signal is an “opt-out preference signal” that must be processed under the Proposed Regulations. For example, the Proposed Regulations do not describe what *content* of a signal would convey a consumer’s intent. As a further example, the Global Privacy Control (“GPC”) header field is “Sec-GPC” with the only available value being “1”.¹ It is unclear how a business would know what to do with that information in the abstract and distinguish it from any number of other irrelevant header fields.

Second, it is unclear what formats are “commonly used and recognized by businesses,” or when a new format would cross the threshold to become a format “commonly used and recognized by businesses.” While the ISOR suggests that the GPC is a “commonly used and recognized by businesses” (ISOR at 33), the Agency provides no evidence supporting this assertion. Because there is no “commonly used and recognized” format for opt-out preference signals, the Agency

¹ <https://globalprivacycontrol.github.io/gpc-spec/#the-sec-gpc-header-field-for-http-requests>

California Privacy Protection Agency
Mr. Brian Soublet
Page 5

should not make honoring such signals required until after issuing actionable technical specifications and allowing time for tools to become available on the market for businesses to implement such specifications.

Third, the Proposed Regulations provide no clear path to compliance for businesses that do not offer their services via webpage, for example businesses that offer connected devices and OTT services. HTTP header fields are not necessarily compatible with OTT devices and there is no “commonly used and recognized” opt-out preference signal format within the OTT device industry.

(ii) Businesses have no reasonable means of assessing what information was provided to consumers when configuring opt-out preference signals.

Section 7025(b)(2) of the Proposed Regulations provides that “[t]he 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.” Businesses receiving opt-out preference signals have no control over what the opt-out preference signals communicate to consumers, and the Agency does not have authority over the providers of the “platforms, technologies, or mechanisms” that send such signals. It is unclear how businesses will be able to determine whether consumers sending opt-out preferences signals actually received such notice from platforms, technologies, or mechanisms. The Proposed Regulations provide no guidance on how to comply with this requirement.

4. The Proposed Regulations fail to address specific requirements that the CPRA delegated to the Agency with respect to opt-out preference signals.

Despite a clear mandate to do so under Section 1798.185(a)(19) of the CPRA, the Proposed Regulations fail to provide specifications and requirements for opt-out preference signals with respect to (i) limiting the use or disclosure of sensitive personal information or (ii) conveying that the consumer is less than 13 years of age, or at least 13 years of age and less than 16 years of age (collectively, “Additional Opt-Out Signal Requirements”). The Agency conceded in the ISOR that it failed to address the Additional Opt-Out Signal Requirements, and it explained that it did not address them for three reasons, each of which suggests that Section 7025 of the Proposed Regulations is not sufficiently complete to be adopted. *See* ISOR at 33.

First, the Agency explained that it did not address the Additional Opt-Out Signal Requirements in an effort to reduce the burden on businesses to respond to differing signals. *Id.* Issuing an incomplete set of regulations will not reduce businesses’ burdens, however, because, rather than expending resources once to implement a solution that complies with all of the options

California Privacy Protection Agency
Mr. Brian Soublet
Page 6

contemplated by the statute, businesses will instead be required to devise a way to comply with the limited vague requirements in the Proposed Regulations and expend more resources later whenever the Agency issues regulations to patch in the additional opt-out signals. Rather than reducing burdens on businesses, the Agency's haphazard and incomplete approach increases them.

Second, the Agency explained that it did not address the Additional Opt-Out Signal Requirements because no mechanism currently exists to communicate the expression of these rights. *Id.* The absence of such a mechanism is not surprising, however, because the Agency has not yet issued any technical specifications defining such a mechanism. The Agency must first solicit broad public participation to develop technical specifications for the Additional Opt-Out Signal Requirements before any implementing mechanism can be expected to exist.

Third, the Agency explained that it did not address the Additional Opt-Out Signal Requirements in order to prioritize the Agency's limited resources in promulgating regulations as quickly as possible as required by the CPRA amendments. *Id.* A need to promulgate regulations "as quickly as possible," however, does not provide an adequate basis for imposing incomplete regulations on businesses that will inevitably have to be updated by the Agency and thereby imposing undue burdens on businesses through vague and eventually obsolete requirements.

Because the Proposed Regulations fail to comply with their statutory mandate, and in order to avoid the unnecessary expenditure of resources by businesses to comply with a regulatory requirement that lacks sufficient specificity to allow businesses to comply with the regulations, the Agency should withdraw Section 7025 of the Proposed Regulations until it can be replaced with regulations that comply with the statutory requirements.

5. Contrary to Section 7025(b)(2) of the Proposed Regulations, the opt-out preference signal should require the consumer to indicate their state of residence and that information should be transmitted as part of the signal.

Section 7025(b)(2) of the Proposed Regulations provides that "[t]he configuration or disclosure [of the opt-out preference signal] does not need to be tailored only to California or to refer to California." The opt-out preference signal *should* be tailored to California, however, because the specifics of the opt-out rights provided by the CPRA are unique to California. If a business does not know the state of residence of the consumer sending the opt-out preference signal, the business will not know with which state's statutory and regulatory requirements apply to the consumer's request.

While California, Colorado, and Connecticut are currently the only states with opt-out preference signals contemplated by their respective general privacy laws, there are already

California Privacy Protection Agency
Mr. Brian Soublet
Page 7

substantive differences in the types of opt outs each state provides. Furthermore, other states are likely to follow suit with their own opt-out signals, which will inevitably create further divergence in compliance requirements. Meanwhile, the CPRA, Colorado Privacy Act, Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313 (“ColoPA”), and Connecticut Personal Data Privacy and Online Monitoring Act, Public Act No. 22-15 (“CPOMA”) each require that consumers be informed about the opt-out choices available to them.

Nevertheless, opt-out preference signals are likely to be transmitted in circumstances where the business does not know the actual identity of the consumer, let alone the consumer’s state of residence. It is thus important for platforms sending opt-out preference signals to be able to know the consumer’s state of residence to present the correct opt-out choices to the consumer, and for businesses receiving opt-out preference signals to know the same to apply the correct opt-out rights.²

The ISOR states that the platform, technology, or mechanism transmitting the opt-out preference signal need not explicitly reference California because doing so “would be burdensome to businesses because it would reduce the interoperability of a universal signal and require state-specific implementation, which is unnecessary given that the sale or sharing of personal information is not unique to any individual State or jurisdiction. Furthermore, binding the signal to a specific State is not necessary because it is merely legal in nature and not required for functionality.” ISOR at 34. Such justification is simply not true. California’s opt-out rights and requirements are unique to the state, and not knowing the consumer’s state of residence makes it unclear to the business which state’s laws apply. Moreover, states have different definitions of “sale” and no other state has adopted the CPRA’s definition of “sharing.”

The ISOR goes on to state that “[i]f a business treats consumers differently depending on the state that they reside in, they can seek this information in response to the signal.” *Id.* This option, however, is unnecessarily burdensome for both businesses and consumers. Consumers should be able to provide their state of residence *once* when configuring their opt-out preference

² Requiring a consumer to provide their state of residence to be transmitted as part of the opt-out signal is consistent with the requirement in Section 1798.185(a)(19)(A)(ii) of the CPRA that the regulations “[e]nsure that opt-out preference signal . . . does not require that the consumer provide additional information beyond what is necessary” because, as explained above, knowing the consumer’s state of residence is necessary to ensure that the business is able to apply the correct opt-out rights to the signal received. Furthermore, knowing the consumer’s state of residence is also necessary to “[e]nsure that the opt-out preference signal [for California] does not conflict with other commonly used privacy settings or tools that consumers may employ,” as required by Section 1798.185(a)(19)(A)(iv), such as opt-out preference signals employed for Colorado, Connecticut, or other states.

California Privacy Protection Agency
Mr. Brian Soublet
Page 8

signal and should not need to provide their state of residence for every different business with which they interact. Furthermore, many businesses receiving an opt-out preference signal may have no way of interacting with the consumer to seek this information (particularly where the business is acting as a third party), and thus will not be able to reasonably determine which state's law to apply.

6. The Agency should work with the Colorado Attorney General to create an interoperable technical standard for opt-out preference signals.

Section 6-1-1313(2)(e) of the ColoPA requires the Colorado Attorney General, by July 1, 2023, to “[a]dopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the United States.” Given that the CPRA regulations will most likely precede the ColoPA’s regulations, it would be prudent for the Agency to work with the Colorado Attorney General to ensure that the technical requirements for the CPRA’s opt-out preference signal do not inherently conflict with an opt-out preference signal that could be adopted under the ColoPA.

In particular, by adopting our recommendation that the opt-out preference signal require the consumer to indicate their state of residence and to transmit that information as part of the signal, remaining parts of the signal could be used to indicate an opt-out preference specific to each state’s requirements without having to transmit separate signals for each state. Additionally, allowing for a single header (or other format) signal that is adaptable for each state’s requirements will help avoid situations where a business receives multiple opt-out preference signals from a single consumer that potentially conflict with one another by consolidating the possible signals into a single value.

7. Businesses should be permitted to deny an opt-out preference signal *without* providing notice and an explanation to the requester where the business has a good-faith, reasonable, and documented belief that the request is fraudulent.

In response to a request to opt out of the sale or sharing of personal information, Section 7026(e) of the Proposed Regulations requires businesses to “inform the requestor that it will not comply with the request and . . . provide to the requestor an explanation why it believes the request is fraudulent.” This notice and explanation requirement should not apply when a business receives fraudulent requests through opt-out preference signals. Where a business receives a fraudulent opt-out request purely through a preference signal, there may be no practical way for the business to reply with a notice and explanation because, for example, the business may have no means to send messages to the source of the signal or the fraudulent requests may be coming

**WILSON
SONSINI**

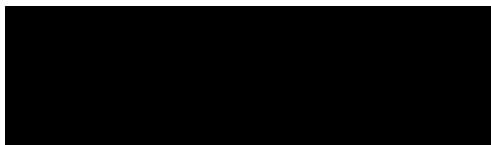
California Privacy Protection Agency
Mr. Brian Soublet
Page 9

in great quantities, such as when bots are used to spam a business with requests that impersonate consumers.

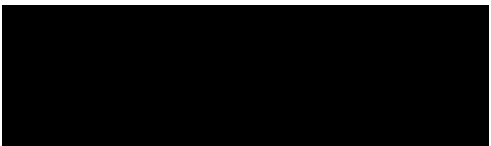
The requirements that businesses have good-faith, reasonable, and documented beliefs will sufficiently effectuate the purpose of this provision, notwithstanding a limited carve-out for the notice and explanation requirements for opt-outs received via fraudulent opt-out preference signals.

Sincerely,

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation



Tracy R. Shapiro



Eddie Holman

From: **Jarrell Cook** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
CC: **Chandler C. Morse** [REDACTED]; **Andrea Deveau** [REDACTED]; **Alicia Priego** [REDACTED]
Subject: Workday | CPHA Public Comment - June 8 CPRA Regulations
Date: 23.08.2022 23:44:26 (+02:00)
Attachments: Workday CPRA comments v3 (submitted).pdf (5 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Attached please find Workday's comments on the proposed CPRA regulations. Thank you for the opportunity and please feel free to reach out at any time.



Workday Comments on the California Privacy Rights Act Draft Regulations

August 23, 2022

Workday is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics have been adopted by thousands of organizations around the world and across industries—from medium-sized businesses to more than 50% of the *Fortune* 500.

Workday is pleased to have the opportunity to provide preliminary comments on the draft regulations governing compliance with the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA) of 2020. We sincerely appreciate the California Privacy Protection Agency's consideration of our comments and the welcoming of public participation in the regulatory process. Our comments focus on the following areas: service provider requirements (including contracts and audits), the importance of preserving the service provider distinction, and considerations regarding business-to-business and employment-related data.

Our previous comments to the proposed rulemaking under the California Privacy Rights Act of 2020, which can be found [here](#), focused on definitions and categories, cybersecurity audits, risk assessments, and automated decision-making. We have focused these comments on incremental considerations related to the California Privacy Protection Agency's draft regulations and look forward to future opportunities to address other categories when the Agency pursues future regulations.

I. Contract Specificity Requirement

The California Privacy Protection Agency (“the Agency”) should provide additional details (or an illustrative example) on the level of specificity required in the written contract with service providers regarding the “specific business purposes and services.”

As a leading service provider of enterprise software applications, Workday has executed written contracts with businesses globally. These contracts describe the Workday services that businesses provide. It is important that these contracts enable us to meaningfully and efficiently provide additional services within the scope of our role as a service provider.

It is costly and complex to negotiate thousands of contracts to add additional requirements. As such, at a minimum, the Agency should clarify the level of specificity required in written contracts between businesses and service providers. This will enable service providers like Workday to assess how to best balance the required level of specificity with the flexibility to expand the scope of services provided as necessary, while remaining in compliance with privacy and data protection laws.

Recommendation #1: *Clarify the level of specificity required in the written contract with service providers regarding the “specific business purposes and services” in §7050(b)(2)¹ and §7050(a)(2). See relevant sections in footnote.²*

II. Data Use Restrictions

The Agency should clarify that “combining or updating personal information received from the business with personal information that it received from another source” in § 7051(a)(5) is allowed for improving the service. We assume the intent of this section is to prohibit the use of this data for targeted ads, rather than general product development or improvement. The Agency should clarify that businesses, including service providers, are permitted to use or combine data to create new and better services when those activities do not directly monetize consumers’ personal information, such as for advertising.

The Agency should also clarify that the language “unless expressly permitted by the CCPA or these regulations” includes the exceptions listed in § 7050(b)(1-4), particularly “internal use by the service provider to build or improve the quality of its services”, as outlined in § 7050(b)(4). Building effective machine learning technology depends on large amounts of data being ingested by a machine learning model. While the CPRA sought to restrict the use of data to prevent undisclosed consumer profiling, it did not intend to inhibit the adoption and use of machine learning in general or internal uses of data by a service provider that do not impact individuals’ privacy, but are used to improve products and services. As such, it is important for the Agency to clarify that this prohibition does not extend to important exceptions under the CCPA.

In addition, the Agency should consider clarifying, perhaps by adding an illustrative example, that the prohibition on combining or updating of personal information does not apply once the personal information is aggregated, as that information is—by definition—no longer personal information.

Recommendation #2: *The Agency should add language clarifying the scope of the data use restrictions (if any) outlined in § 7051(a)(5). See proposed language in footnote.³*

¹ “A service provider or contractor shall not retain, use, or disclose personal information in the course of providing services except... (2) For the specific business purpose(s) and service(s) set forth in the written contract required by the CCPA and these regulations.”

² “The contract required by the CCPA for service providers and contractors shall...(2) Identify the specific business purpose(s) and services(s) for which the service provider or contractor is processing personal information on behalf of the business and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified business purpose(s) set forth within the contract. The business purpose or service shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.”

³ “The contract required by the CCPA for service providers and contractors shall...(5) “Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information received from, or on behalf of, the business with personal information that it received from another source [to provide targeted ads] / [unless expressly permitted by the CCPA or these regulations, [including as provided in section § 7050(b)(1-4)].

III. Compliance Audits

The Agency should tailor the scope of the compliance audits businesses can request from service providers to account for practicality and the cost and burden on service providers. The Agency should allow the service provider to respond to requests for audits and remediations with already-existing documentation, including third party audits and certifications.

The Agency may also consider softening the prescriptiveness of what constitutes “reasonable and appropriate steps” in (a)(7). As written, it lacks the flexibility to factor in complex and evolving technology—including service provider environments that may, for example, prohibit external system scans for data security and privacy purposes.

Recommendation #3: *The Agency should revise § 7051(a)(7) to add the ability for service providers to respond to requests with already existing documentation, including existing third party audits and certifications which demonstrate regular scans occur. See proposed language in footnote.⁴*

IV. Data Transfers to Service Providers

The Agency should add language to § 7051(c) to clarify that disclosure of information to another party would not constitute a “sale” or “share” simply because the written contract with the service provider is deemed to insufficiently cover a required aspect under the CPRA.

A service provider that is operating in its capacity as a service provider, should not—but for a technical failure to include one or more sufficient provisions in its contract with a business—have to acquiesce its position as a service provider because it becomes a recipient of shared or sold personal information. Rather, the transfer of information would still need to independently meet the requirements of the defined terms “sale” or “share.”

Recommendation #5: *The Agency should add clarity that a disclosure of information pursuant to a contract that fails to satisfy service provider contractual provisions must still satisfy the requirements of the terms “sale” or “share” to constitute such an action. See proposed language in footnote.⁵*

⁴ “The contract required by the CCPA for service providers and contractors shall... (7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it received from, or on behalf of, the business in a manner consistent with the business’s obligations under the CCPA and these regulations . Reasonable and appropriate steps may include ~~ongoing manual reviews and automated scans~~ of the service provider’s ~~already-existing assessment documentation, including third party audits and certifications, such as a SOC 2 report or ISO certifications that demonstrate the service provider conducts regular assessments, audits, or other technical and operational testing at least once every [24 months, or more frequently as mutually agreed upon by the parties].~~

⁵ “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 ~~[provided the disclosure of personal information falls within the definition of the applicable term, respectively].~~”

V. Due Diligence Requirement

The Agency should streamline the requirements on service provider due diligence in § 7051(e). In particular, the Agency should consider striking the illustrative example as redundant because the concept is captured in the first sentence that states that whether the business conducts due diligence is a factor in the business' reason to believe that there is potential noncompliance. Furthermore, as written, the example could be read as requiring businesses to conduct regular audits on their service providers in order to rely on this defense, even if there is no reason to believe the service provider is not in compliance.

As a service provider working with thousands of businesses globally, the requirement to administer and facilitate audits for every business solely to enable these businesses to rely on this defense would be cost prohibitive and impractical. In particular, it would require service providers to reallocate resources designated for building meaningful compliance programs to facilitate arbitrary audits to prove the robustness of the program absent any indication of noncompliance.

Recommendation #6: *The Agency should remove the example provided in § 7051(e) regarding service provider due diligence requirements. See proposed language in footnote.⁶*

VI. Service Provider Distinctions

The Agency should ensure the protections and distinctions in § 7050(d) remain intact. Workday is a service provider to the extent it provides software applications to businesses, and the businesses interact directly with its end consumers, business-to-business contacts, or employees. Indeed, we have invested significant resources and staff in building our online portal to triage CCPA requests based on the individual's affiliation with Workday. Since most consumers submit CCPA requests to Workday in our capacity as a service provider, we typically refer them to the business they are affiliated with to act upon their request (to the extent we cannot, or our agreement with the business directs us otherwise).

Our business customers and consumers look to us to help them comply with these CCPA requests, and have generally found our portal and this process straightforward and user-friendly. It is important that this critical provision and distinction from third parties remains intact for service providers like Workday who continue to help businesses comply with CCPA/CPRA and are not in the business of selling data.

Recommendation #7: *Recognize the importance of key service provider distinctions by ensuring the protections and distinctions in § 7050(d) remain intact.*

⁶ 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 nor exercises its rights to 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."~~

VII. Employment-Related Information

The Agency should clarify within the definition of employment-related information that this type of data is generally exempt from certain requirements of the CPRA, particularly given it may be subject to existing state and federal laws.

At present, employment-related data is exempt from the CCPA. However, this exclusion sunsets in 2023. The drafters of the CCPA and the CPRA recognized that certain data is collected and used differently than consumer data. For example, employment-related data is not generally used for marketing, is collected often to comply with laws or fulfill contracts with employees, and often must be kept after the end of the employment relationship to comply with various requirements. The provisions of the CCPA/CPRA may conflict with these obligations in some cases. Where rights under existing laws may not directly conflict with various rights under the CPRA, those rights may implement significant additional organizational churn, for little gain, due to existing practical and requirements in the legal relationship between employers and employees.

Recommendation #8: *The Agency should clarify within the definition of employment-related information in § 7001(j) that this type of data is explicitly exempt from aspects of the CPRA. See proposed language in footnote.⁷*

* * *

Workday appreciates the opportunity to comment on the Agency's draft regulations implementing the California Privacy Rights Act of 2020. If you have any questions or if we can provide additional information, please do not hesitate to contact Jarrell Cook, Senior Manager, State and Local Government Affairs, at [REDACTED]

⁷ (j) "Employment-related information" means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (m)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose. [To the extent employment-related information is used for the purposes enumerated in § 7027(l)(1-7), it shall be exempt from the right to delete and right to know].

From: **Justin Brookman** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 19:46:48 (+02:00)
Attachments: CPPA regs comments (summer 2022).pdf (14 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find Consumer Reports's comments on the Text of Proposed Regulations.

This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.

Comments of Consumer Reports
In Response to the
California Privacy Protection Agency
Text of Proposed Rules under the California Privacy Rights Act of 2020

By

Justin Brookman, Director of Technology Policy

August 23, 2022



Consumer Reports¹ appreciates the opportunity to comment on the proposed rules (the Draft Regulations) interpreting the California Privacy Rights Act (CPRA).² We thank the California Privacy Protection Agency (CPPA) for soliciting input to make the California Consumer Privacy Act (CCPA),³ as amended by Proposition 24, work for consumers.

Overall, we are very supportive of the Draft Regulations. They build upon the existing CCPA regulations to deliver strong protections for California consumers. We appreciate the long and difficult work that went into creating these regulations, including incorporating the feedback of dozens of stakeholders, including Consumer Reports.⁴ We make the following comments to urge additional improvements to the text, or in some cases to urge the CPPA to resist calls to revise provisions contained within the Draft Regulations.

I. OPT-OUT PREFERENCE SIGNALS

Opt-out Preference Signals (OOPSs) are functionally necessary to make an opt-out based law work. Consumer Reports's investigations into the practical implementation of the California Consumer Privacy Act has found that too many companies have failed to adhere to the letter and spirit of the CCPA, and consumers have run into innumerable difficulties when attempting to individually opt out of the sale of their information under the CCPA.⁵ As consumers cannot practically opt out at every one of the hundreds, if not thousands, of companies that sell consumer data, the CPPA must provide clarity as to how companies should adhere to OOPSs to make the exercise of consumer rights meaningful for California citizens.

¹ Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

² California Privacy Protection Agency, Notice of Proposed Rulemaking, (Jul. 8, 2022), https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf.

³ For purposes of this comment, we will refer to the current text of California's privacy law — as amended by the CPRA — as the CPRA. References to the CCPA are references to the original CCPA before it was amended.

⁴ Justin Brookman, Maureen Mahoney, and Nandita Sampath, Comments of Consumer Reports In Response to the California Privacy Protection Agency Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21), Consumer Reports, (Nov. 8, 2021), [hereinafter "Consumer Reports Initial Comments on CCPA Rulemaking"] <https://advocacy.consumerreports.org/wp-content/uploads/2021/11/Consumer-Reports-CPRA-Comments-No.-01-21-11.08.21.pdf>.

⁵ Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

A. Mandatory Adherence to OOPSs

First and fundamentally, we support the clarification in § 7025(e) of the Draft Regulations that companies are required to adhere to OOPSs regardless of whether they comply with § 135 of the CPRA in a frictionless manner or not. As we describe in more detail in our previous comments to the CPPA,⁶ making compliance with OOPSs optional would weaken existing privacy protections in California, and run counter to both the language and intent of the CPRA. In order to function effectively, opt-out regimes need global opt-out options; for global opt-out options to function effectively, companies must be required to adhere to them. Fortunately, § 135(e) of the CPRA is quite clear that companies must adhere to OOPSs regardless of whether they comply with § 135(a) or § 135(b) of the law:

A consumer may authorize another person to opt-out of the sale or sharing of the consumer’s personal information . . . including through an opt-out preference signal . . . indicating the consumer’s intent to opt-out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer’s behalf . . . regardless of whether the business has elected to comply with subdivision (a) or (b) of this Section.

If the CPRA is interpreted counterintuitively to not require adherence to universal signals, the law will be a failure and Californians will not have the ability to practically limit the sharing or selling of their data. Our strongest recommendation to the CPPA is to retain the requirement that companies must honor opt-out requests sent through OOPSs.

B. OOPS Registry

As we previously recommended in our oral testimony before the CPPA on May 5th of this year, we recommend that the CPPA create and regularly update a registry of signals and settings that should be treated as legally binding opt-out requests under the CPRA. Having a definitive registry would provide more clarity to consumers and businesses than the Draft Regulations’ standard which only says that OOPSs “shall be in a format commonly used and recognized by businesses” and that the signal clearly is “meant to have the effect of opting the consumer out.”⁷ While § 7025(b)(1) lists “an HTTP header field” as an example of a commonly-used format, it is unclear if *any* HTTP header — no matter how widely used — created by a developer with the intent of opting users out must be treated as valid request. Offloading to companies the responsibility for judging whether signals are valid introduces unnecessary ambiguity that bad-faith actors may exploit to frustrate the effectiveness of OOPS.

⁶ Consumer Reports Initial Comments on CPPA Rulemaking, pp. 4-6.

⁷ Draft Regulations § 7025(b).

The initial experience of compliance with the CCPA shows that many companies will indeed take advantage of any potential loopholes to get around the law's substantive restrictions.⁸

Creating and maintaining such a registry is readily feasible, as there are a limited number of platforms and settings that could plausibly qualify as OOPSs at present. For ease of compliance, the list should be relatively stable and slow-changing over time, and so maintaining the list would be practical even if each new addition is contingent upon approval by the CPPA board. As new OOPSs are added to the list, the CPPA could give companies a grace period — such as six months — before it will take enforcement action against companies for failing to comply with the signal. This would give companies a reasonable amount of time to configure their systems in order to respond to the new signal.

The Global Privacy Control, a web-based OOPS with over 50 million unique users each month, should be one of the OOPSs designated as conveying a legally binding request to opt out of the sharing or selling of a user's personal information.⁹ The Global Privacy Control has already been recognized by the California Attorney General as legally binding under the CCPA;¹⁰ the CPPA should update its guidance to consumers and companies — as part of a registry or otherwise — that GPC signals remain valid opt-out signals under the CPRA.

In assessing which privacy controls should be interpreted as sending legally enforceable OOPSs, the CPPA should broadly consider any settings as legally valid opt-outs that are roughly consistent with a consumer intent to limit data sharing or cross-site targeted advertising. This would allow California's law to be interoperable with Colorado, Connecticut and other emerging state privacy laws, all of which define opt-out rights slightly differently (Colorado's privacy law, for example, affords consumers two different opt-out rights for data sales (but not sharing) and the use of information for "targeted advertising"). OOPSs should not have to articulate a sprawling and ever-evolving boilerplate of all possible rights to be invoked; instead they should reasonably be interpreted as exercising the rights associated with the behaviors intended to be addressed by the OOPS.

Regardless of whether the CPPA adopts an OOPS registry, companies should be transparent about which OOPSs they adhere to, and for which jurisdictions. We recommend the CPPA revise § 7011(e)(3) to require companies to within their privacy policies specifically

⁸ Maureen Mahoney, *Many companies are not taking the California Consumer Privacy Act seriously—the attorney general needs to act* (Jan. 9, 2020), Consumer Reports Digital Lab, <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>; Wendy Davis, *Some Advertisers See Loopholes In California Privacy Law*, MediaPost, (Oct. 29, 2019), <https://www.mediapost.com/publications/article/342338/some-advertisers-see-loopholes-in-california-privacy-law-115828>

⁹ Global Privacy Control, <https://globalprivacycontrol.org/>. Consumer Reports is a founding member of the Global Privacy Control initiative and regularly participates in the management of the protocol.

¹⁰ California Consumer Privacy Act, Frequently Asked Questions, <https://oag.ca.gov/privacy/ccpa>.

identify the OOPSs they treat as valid opt-out requests under the CPRA. Such a requirement will provide needed transparency and accountability from companies and go a long way towards making OOPSs reliable for consumers. We also support the CPPA's proposal to display to users their opt-out state so they can know whether their opt-out requests are being honored (see *infra* § I.D, Re-opt-in).

C. Scope of OOPS opt-out

The CPPA should make more clear that when a user's real-world identity is known to a company, OOPSs and other opt-out requests should apply in other scenarios where the company is able to identify that user. This result is implied by § 7025(c)(1) which states that companies must treat OOPSs as a valid opt-out request for "that browser or device, and, if known, for the consumer," as well as the examples provided in § 7025(c)(7)(B) and (C). However, to avoid any ambiguity, the text should be explicit that companies that receive an online request to opt out of data sale or sharing should propagate that opt-out to other contexts as well if the user is identified by the service by an identifier that applies in those other contexts.

Similarly, § 7026 of the Draft Regulations should clarify that manual opt-out requests on a website should also be applied universally when a user is known to the company. However, if the company is only tracking on a pseudonymous basis (such as a cookie), it need not collect more information in order from the user in order to apply the opt-out in other contexts.

We support the language in § 7025(c)(2) stating that companies may optionally ask users if they would like to provide additional information solely to effectuate their opt-out to other contexts where the user is known to the company, and we suggest that comparable language be added to § 7026 as well. Companies can make the choice about whether such a prompt would detract from the overall consumer experience, but if offered, it could provide a means to make the consumer's opt-out choice more effective for that particular service.

Finally, while there have been several efforts to develop OOPSs that apply to online data sharing, there has been less attention paid to equivalent offline OOPS mechanisms. While some online OOPS are already sufficiently robust to be recognized as conveying binding opt-out requests, the CPPA should explore and invite comment on approaches to implement offline approaches. One potential solution would be for the CPPA to create and house a Do Not Sell registry, modeled on the popular Do Not Call registry, that businesses would be required to check before selling consumer data tied to those identifiers. The CPPA would collect consumers' identifiers, such as emails and phone numbers, and companies would pay in order to consult the list (thus ensuring that companies seeking to sell data would absorb the costs for the operation of the website). Consumers could add their identifiers to the registry through a public portal, much like Do Not Call. This would enable consumers to easily and globally express their preferences

to opt-out of the sale of data tied to specific identifiers (or hashes of specific identifiers). Companies would be required to check this database before disclosing or tracking based on consumers' information, much as they do today for the Do Not Call registry. The Do Not Call registry currently includes 244.3 million active registrations, indicating that this is an easy way for consumers to opt out of telemarketing messages.¹¹ On the other hand, compliance with Do Not Call has been inconsistent given the ease of creating difficult-to-trace voice-over-internet calls. One downside of a registry approach would be to make such identifiers publicly available to bad faith actors and more susceptible to spam. The rule would need to be paired with aggressive enforcement as well as technical measures to remediate registry access and misuse.

D. Re-opt-in

Despite the use of an OOPS, some consumers may still want the ability to grant permission to individual sites and services to sell their data or to engage in cross-site targeted advertising. However, this seems unlikely to be the norm. Unlike rights such as access and deletion where consumers' choices are likely to be heterogeneous, a consumer who generally does not want their data sold likely wants *no one* to sell their data — this is the reason for which OOPSs were created under California law.

In practice, a provision allowing for consumer re-opt-in will primarily empower companies to pester users into granting permission to ignore the OOPS. Many (if not most) companies confronting the ePrivacy Directive and Global Data Privacy Regulation in Europe adopted just this approach to a consent requirement for tracking: rather than limit their data processing to what was functionally necessary in response to the law, they instead bombarded consumers with overwhelming, confusing, or downright abusive interfaces to simulate consent to maintain the status quo of data sharing and ad targeting.¹²

If the functional result of using an OOPS is simply that every site or app will then harass you for permission to ignore, the controls will end up being ineffective failures for California consumers. For this reason, there is a strong policy argument to *prohibit* re-opt-in to ignore OOPSs under the CPRA since the costs of re-opt-in (hassle, user experience, inadvertently granting consent) will almost certainly outweigh the benefits to the narrow slice of consumers who want to make targeted exceptions to a universal opt-out choice. However, such a blanket prohibition is likely disallowed by the structure of CPRA, which only prohibits companies that do not post a “Do Not Sell or Share My Personal Information” link on their site from interrupting

¹¹ National Do Not Call Registry Data Book FY 2021, Fed. Trade Comm’n at 5, (Nov. 2021), <https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2021>. The efficacy of the DNC registry is also limited by the fact that it only applies to telemarketing, and that it does not hinder scammers, debt collectors, and others in their communications.

¹² Jennifer Bryant, *Belgian DPA fines IAB Europe 250K euros over consent framework GDPR violations*, IAPP, (Feb. 2, 2022), <https://iapp.org/news/a/belgian-dpa-fines-iab-europe-250k-euros-over-consent-framework-gdpr-violations/>.

the user experience to ask for permission to ignore the OOPS. Companies that choose to adhere to § 135(a) of the CPRA are not so constrained.

Unfortunately, we do not believe that the inducement of not posting a “Do Not Sell or Share My Personal Information” link will be sufficient inducement to companies to refrain from asking for consent to ignore OOPSs. As such, the CPPA should take steps to ensure that Californians who use an OOPS to exercise their legal rights are not inundated with relentless and confusing requests to sell or share in contravention of the OOPS.

At the very least, the CPRA should disincentivize unwanted nudges, require a high standard for consent for re-opt-in, and aggressively constrain the use of dark patterns to subvert user intentions (*see infra*, § II, Consent and Dark Patterns). Indeed, the standard for re-opt-in should be higher than the standard for ordinary consent, as the user has already communicated a general preference to not have their data sold or shared. Section 7025 of the Draft Regulations provides precise rules for companies that adhere to the “frictionless” compliance path for OOPS under § 135(b) of CPRA; the CPPA should also provide heightened rules for what degree of “friction” is allowable under § 135(a) beyond the consent rules laid out in §§ 7004 and 7028. We support the two-step re-opt-in process laid out in § 7028 but recommend the CPPA consider additional protections, such as requiring that the prompt defaults to disallowing consent (consistent with the consumer’s general stated preference) and specifying the language that should be used to convey consistently and fairly to consumers what is being requested. We also recommend clarifying that when a user denies consent to ignore a general OOPS, the company cannot ask again for the next 12 months. A general prohibition on asking for re-opt-in is laid out in § 7026(j) — that language should be added to § 7025 as well to be clear that that rule applies to OOPS opt-outs as well.¹³

We support the general framework laid out in the Draft Regulations for handling contradictory indications of user intent: In the event that a newly invoked OOPS setting contradicts an earlier permission to engage in targeted advertising or data sales, the newer OOPS setting should control.¹⁴ At this point, a company may ask for consent to engage in targeted advertising or data sale notwithstanding the general preference articulated by the OOPS. If the user’s consent is consistent with the heightened requirements for re-opt-in, then it may be reasonable to allow the company to prospectively disregard the general OOPS setting unless and until they revoke the specific exception granted to the company.

¹³ It is not entirely clear from the current text how many of the requirements laid out for opt-outs in § 7026 also apply to opt-outs communicated by an OOPS. If all the requirements apply, the text should make that clear. In addition to a prohibition on asking for re-opt-in, other elements of § 7026 should apply to certain OOPS opt-outs as well. For example, they should adhere to the requirements laid out in § 7026(f) to notify downstream third-parties of the opt-out choice. Draft Regulations § 7026(f)(B)-(C).

¹⁴ Draft Regulations, § 7025(c)(3).

Given the significant potential for abuse, we also support language in the Draft Regulations that companies should be required to respond to OOPSs with a prominent and persistent notice about the user's opt-out or re-opt-in state.¹⁵ A user would then always be able to see if their opt-out preferences were being honored, and could take steps to adjust their settings if they were different than expected. Alternatively, the CPPA could provide that consumers should be able to assume that OOPS controls are operative, and only companies that disregard an OOPS control — either because the company believes it has re-opt-in consent or because it does not believe the signal conforms to the CPRA's requirements for an OOPS — must provide prominent notice to consumers that the OOPS is not considered operative. This approach would incentivize companies to respect OOPS signals and disincentivize bad faith efforts to generate spurious consent.¹⁶ For either of these approaches, a company providing notice that an OOPS is being disregarded should include clear instructions on how to remedy a defective setting or how to revoke consent if the consumer so desires.

II. CONSENT AND DARK PATTERNS

Subverting consumer intent online has become a real problem, and it's an important issue for regulators to address. In response to Europe's recent GDPR privacy law, many websites forced users through confusing consent dialogs to ostensibly obtain consent to share and collect data for any number of undisclosed purposes.¹⁷ And researchers increasingly have been paying attention to manipulative dark patterns as well. A 2019 Princeton University study of 11,000 shopping sites found more than 1,800 examples of dark patterns, many of which clearly crossed the line into illegal deception.¹⁸ Consumer Reports research has also identified numerous dark patterns, including in smart TVs, food delivery apps, and social media.¹⁹ For example, CR testers found that for all of the smart TVs examined, a consumer moving quickly through the television

¹⁵ Draft Regulations, § 7025(c)(3)-(6).

¹⁶ This protection could be supplemented with the requirement we suggested earlier that § 7011(e)(3) should be revised to require companies to specifically identify the OOPS signals they adhere to in their privacy policy. See *supra* § I.B, OOPS Registry.

¹⁷ *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018), <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

¹⁸ Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proc. ACM Hum.-Comput. Interact. (2019), <https://webtransparency.cs.princeton.edu/dark-patterns/>.

¹⁹ *Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds*, CONSUMER REPORTS (Feb. 7, 2018), <https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-find>; *Collecting #Receipts: Food Delivery Apps and Fee Transparency*, CONSUMER REPORTS (Sept. 29, 2020), https://digital-lab-wp.consumerreports.org/wp-content/uploads/2020/09/Food-delivery_-_Report.pdf; Consumers Union Letter to Fed. Trade Comm'n (Jun. 27, 2018), <https://advocacy.consumerreports.org/wp-content/uploads/2018/06/CU-to-the-FTC-Facebook-Dark-Patterns-6.27.18-1-1.pdf>; *Consumer Reports Calls On FTC to Take Tougher Action to Stop Hidden Resort Fees*, CONSUMER REPORTS (Aug. 6, 2019), https://advocacy.consumerreports.org/press_release/consumer-reports-calls-on-ftc-to-take-tougher-action-to-stop-hidden-resort-fees/.

set-up process will end up providing consent to the tracking of everything they watch through automatic content recognition.²⁰ Consumer Reports has helped to collect dark patterns through the Dark Patterns Tipline, a project to crowdsource examples of these deceptive interfaces to help advocate for reform.²¹

We largely support the conditions for consent laid out in § 7004. We urge the CPPA to retain the requirements that consent requests be easy to understand, offer symmetry of choice, avoid confusing elements, and avoid manipulative language or choice architecture.

One additional requirement we suggest is to clarify that requests for consent for data processing must be made in response to a dedicated prompt. That is, any consent for processing should be made pursuant to a standalone interface, separate from any privacy policy, license agreement, or other longform contract, that on its face clearly and prominently describes the processing for which the company seeks to obtain consent.

We recommend two narrow amendments to the “Symmetry of Choice” requirement. First, the text should state that the option to grant consent shall not be more prominent or selected by default; currently, the rule only states that “[t]he path for a consumer to exercise a more privacy-protective option shall not be longer than the path to exercise a less privacy-protective option.”²² While the example in § 7004(a)(2)(D) indicates that a “yes” button may not be more prominent than the “no” button, this principle should be included within the text of the rule itself and not just the illustrative examples. Second, the CPPA should clarify that the option to grant consent may be less prominent or more time-consuming than the option to decline consent. The text of the requirement states that the path to decline consent “shall not be longer” than the path to accept, but the term “symmetry of choice” may present ambiguity. One additional sentence clarifying that the option to decline may be easier to exercise, take fewer steps, be more prominent, or be selected by default would be helpful.

Finally, the CPPA should develop standardized disclosures, so that companies have more clarity about appropriate interfaces and design choices. Given the persistent problems with dark patterns in cookie consent interfaces, which purport to obtain consumers’ consent for any number of inappropriate data uses, the CPPA should develop a model interface — or at least language — for obtaining consent to opt back into the sharing of information, and for obtaining consent for secondary processing of sensitive personal information. Overall, the CPPA should err strongly on the side of clear, simple, bright-line rules instead of vague, debatable standards that

²⁰ *Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds*, Consumer Reports, (Feb. 7, 2018), <https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/>.

²¹ Dark Patterns Tipline, <https://darkpatternstipline.org/>.

²² Draft Regulations, § 7004(a)(2).

could afford bad faith actors too much wiggle room to justify deceptive behavior. If over time the CPPA's exemplary guidance proves insufficient to rein in the use of dark pattern interfaces that subvert consumer intent, the CPPA must be more prescriptive and provide a narrower range of choices and specific language for companies that purport to obtain consent for data processing.

III. NON-RETALIATION

Section 125(b)(4) of the CPRA provides that a “business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.” However, the Draft Regulations provide no clarity as to what practices might violate this provision — instead, they only reiterate § 125(a)(2)'s separate requirement that financial incentives must be “reasonably related to the value provided to the business by the consumer’s data.” We recommend that the CPPA provide examples of behaviors that while satisfying § 125(a)(2)'s requirement nevertheless are prohibited by § 125(b)(4). For example, a provider in a consolidated market without reasonable alternatives should be prohibited *per se* from penalizing consumers for exercising their right to constrain secondary data uses.²³ Similarly, conditioning access to or charging higher prices for certain categories of essential goods and services could also be deemed to be violative of § 125(b)(4).

The Draft Regulations maintain the existing requirement under the CCPA regulations that companies must be able to “calculate a good-faith estimate of the value of the consumer’s data” and “that the financial incentive or price or service difference is reasonably related to the value of the consumer’s data.”²⁴ However, a check of two top loyalty programs suggests that some companies are not actually providing estimates of the value of a consumer’s data, instead offering vague explanations in their disclosures with respect to the overall value of personal information.²⁵ To deter noncompliance with this provision of the law, the CPPA should build on the existing requirement to require companies who make “non-discriminatory” financial incentives to consumers to in the course of making the offer provide access to the required good-faith estimate of the value of the specific consumer’s data.

²³ Consumer Reports Initial Comments on CPPA Rulemaking, pp. 27-28

²⁴ Draft Regulations, § 7080(b).

²⁵ See, e.g., Sephora, Privacy Policy, Notice of Financial Incentive, “The value of your personal information to us is related to the value of the free or discounted products or services, or other benefits that you obtain or that are provided as part of the applicable Program, less the expense related to offering those products, services, and benefits to Program participants.” (August 10, 2022), <https://www.sephora.com/beauty/privacy-policy#USNoticeIncentive>; CVS, Privacy Policy, Financial Incentives, Member Special Information, “For participants in the aforementioned financial incentive programs, the value of the personal information you provide is reasonably related to the value of the financial incentives provided to you. The value of personal information will vary slightly for each member depending on several factors, including but not limited to your interactions and purchases with CVS, the administrative and technical expenses associated with maintaining the ExtraCare program (e.g., IT infrastructure, customer service, marketing strategy & planning), and the extent to which you take advantage of the program’s offerings and discounts (e.g., 2% ExtraBucks rewards for purchases).” (July 18, 2022), https://www.cvs.com/help/privacy_policy.jsp#noticefi.

IV. TRANSPARENCY

Section 7012(g)(3) states that:

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 at the physical location(s) where it is collecting the personal information.

In this case, the mere availability of notice does not seem sufficient: if a third party has the capacity to monitor a consumer within another’s company’s physical place of business, there should be (at the very least) clear signage within the establishment alerting users to this fact (indeed, certain first-party surveillance may be sufficiently invasive to justify signage as well).²⁶ We recommend requiring clear and prominent signage for at least the case of third-party monitoring in physical locations, instead of presenting it as just one possible option under the current Draft Regulations. We also recommend revising the examples provided in §§ 7012(g)(4)(B) and (C) to reflect that change in policy.

V. COMPLAINTS

Section 7300(a)(5) states that formal complaints made to the CPPA must “be signed and made under penalty of perjury.” We recommend deleting this subsection. The threat of criminal prosecution for inadvertently incorrect statements or differing interpretations will chill research and reporting of CPRA violations to the CPPA. Even if a whistleblower does report a violation to the agency, they will be incentivized to provide fewer details lest one happens to be incorrect (or at least disputable). Persons who make complaints to the CPPA do not receive monetary gain or a portion of the CPPA’s relief from a wrongdoer; they are not perversely incentivized to bring bad faith claims to the agency. To the extent the rare complainant is motivated by malice, a company will still have direct recourse against them for defamation and economic interference. While consumers and researchers retain the ability to submit unsigned complaints under § 7301, the CPPA does not have the obligation to respond to a consumer petition submitted in this fashion. Consumers deserve transparency into CPPA decisionmaking without having to subject themselves to potential legal liability. If the CPPA is inundated with bad faith complaints, it could then consider potential consequences against persons who abuse the system or other less burdensome hurdles to filing a formal complaint; until then, the agency should not be deterring others from reporting potential violations.

²⁶ While the Draft Regulations require some degree of notice regarding third-party data collection in physical locations, it is unclear how such monitoring would be consistent with the data minimization and purpose limitation requirements laid out in § 7002. *See infra* § VII, Data Minimization and Purpose Limitation.

VI. RETARGETING

We reiterate our request that the CPPA provide more clarity around the definition of “cross-context behavioral advertising” to ensure that companies do not interpret the term unduly narrowly to largely circumvent its application. The CPPA has the ability under to issue this clarifying rule under § 185(a)(10) of the CPRA which authorizes the CPPA to “issu[e] . . . regulations further defining . . . business purposes” (“cross-context behavioral advertising” operates as an exclusion from the definition of “business purposes”).

The CPRA defines “cross-context behavioral advertising” as:

the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.²⁷

This language arguably is ambiguous when it comes to *retargeting*, which is based on a user’s activity on just one other nonaffiliated website (for example, a user considers buying a pair of Nikes and decides not to — later they see an ad for the same shoes on ESPN). While excluding retargeting from the definition of cross-context targeted advertising would be a tendentious stretch — and most observers have not read the CPRA in this way²⁸ — others have raised doubts as to whether retargeting is covered under the sharing opt out.²⁹ Exempting retargeting — arguably the prototypical example of targeted advertising — from the scope of cross-context behavioral advertising would frustrate consumers and offer a gaping loophole that marketers could take advantage of; the CPPA should specify that targeted ads based on even one nonaffiliated website, application, or online service is still a targeted ad.

²⁷ Cal. Civ. Code § 1798.140(k).

²⁸ See, for example, *Changes to CCPA Put Retargeting in the Regulatory Bullseye*, AD LIGHTNING (Dec. 8, 2020), <https://blog.adlightning.com/changes-to-ccpa-put-retargeting-in-the-regulatory-bullseye>.

²⁹ Arsen Kourinian, *How Expansion of Privacy Laws, Ad Tech Standards Limit Third-Party Data Use for Retargeting*, IAPP (Apr. 27, 2021), <https://iapp.org/news/a/how-the-expansion-of-data-privacy-laws-and-adtech-standards-limits-companies-ability-to-use-third-party-data-for-retargeting/>. (“Major companies are well-positioned to adapt to these developments, as they likely still have a treasure trove of first-party data that they can rely on for retargeting and measuring marketing performance on their owned and operated properties.”) See also *Consumer Retargeting: What’s the Problem?* WIREWHEEL (Jan. 28, 2021), https://wirewheel.io/consumer-retargeting/?utm_medium=Organic-Social&utm_source=Facebook&utm_campaign=2021-02-17-Mark-retargeting-video (Quoting Marc Zwillinger: “I think we are going to get into a much more interesting question when we talk about whether the CPRA prevents retargeting. We may have some different views on that and certainly Alistair McTaggart will probably have a different view.”)

VII. REQUESTS TO OPT OUT AND LIMIT THE USE OF SENSITIVE INFORMATION

We are largely supportive of these sections but offer minor edits. For downstream third-party recipients of opt-out requests, the Draft Regulations should make more clear that they are required to stop processing data they had received related to that consumer unless they become a contractor or service provider of the original business. This requirement is stated in § 7026(f)(3) for third-parties who have continuing access to consumer data, but is not mentioned in § 7026(f)(2) for third-parties who had previously collected such data. The requirement should be added to § 7026(f)(2) as well.

Section 7027(l) provides a list of operational business purposes for which a company does not need to offer consumers a right to limit the use of their sensitive personal information. We recommend adding language to this section clarifying that such processing “shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed.” This would mirror the protection in § 140(e) of the CPRA for permitted business uses to ensure that the processing of sensitive data for these purposes is not excessive.

We also recommend revising the example provided in § 7027(l)(5) regarding contextual advertising. The example currently states that “a business that sells religious books can use information about its customers’ religious beliefs to serve contextual advertising for other kinds of religious merchandise within its store or on its website.” This example is misleading and could introduce unnecessary ambiguity — in this case, the advertisement is being targeted based on the content of the webpage, and *not* necessarily the customers’ religious beliefs. The example should be revised to reflect that.

VIII. DATA MINIMIZATION AND PURPOSE LIMITATION

Finally, we are extremely sympathetic to the data minimization rules laid out § 7002 that constrain secondary use of data beyond reasonable consumer expectations. This is largely consistent with the guidance that we and the Electronic Privacy Information Center laid out in our white paper proposing that the Federal Trade Commission promulgate rules under Section 5 of the FTC Act implementing a data minimization framework.³⁰ We especially note the example provided in § 7002(b)(3) that implies that data sharing — including sharing for advertising purposes — that is not directly related to providing the good or service requested by a consumer is *per se* illegal. It appears that the purpose of § 7002 is to clarify that “the purposes for which the personal information was collected or processed” under § 100(c) of the CPRA are the

³⁰ Consumer Reports and the Electronic Privacy Information Center, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 26, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

purposes of *the consumer* and not whatever purposes are intended by a company with which they are interacting — though that could be more explicit.

However, this promising data minimization principle is undercut by other provisions in the Draft Regulations (and indeed, the CPRA itself). Section 7002(a) states that a company may process data for incompatible purposes “with the consumer’s explicit consent.” However, there is no consent exception to § 100(c) of the CPRA: processing must be

reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

More broadly, it is not clear how the proposed data minimization language intersects with other elements of the Draft Regulations and CPRA, which allows for companies to sell and share data subject only to opt-out rights, and to process data for excepted business purposes with no recourse at all. While we would prefer a regime where most secondary data processing is strictly prohibited, the law should at least be clear as to which set of rules governs which data collection and processing activities.

We thank the CPPA for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Justin Brookman
[REDACTED] for more information.

From: **Jessica Lee** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
CC: **Shely Berry** [REDACTED]
Subject: CCPA Public Comment
Date: 23.08.2022 23:48:50 (+02:00)
Attachments: Loeb Comments - CCPA Proposed Regulations (8.23.22)(22636522.4).pdf (11 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please see the attached on behalf of Loeb & Loeb LLP.

Jessica B. Lee, CIPP/US, CIPP/E, CIPM (She/Her)
Partner, Chair, Privacy, Security & Data Innovations

 Loeb & Loeb

345 Park Avenue | New York, NY 10154

Mobile: [REDACTED] | E-mail: [REDACTED]

Los Angeles | New York | Chicago | Nashville | Washington, DC | Beijing | Hong Kong | www.loeb.com

Jessica Lee
Partner



345 Park Avenue | New York, NY 10154

Direct Dial: [REDACTED] | Fax: [REDACTED] | E-mail: [REDACTED]

Los Angeles | New York | Chicago | Nashville | Washington, DC | San Francisco | Beijing | Hong Kong | www.loeb.com

CONFIDENTIALITY NOTICE: This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify the sender. Please destroy the original transmission and its attachments without reading or saving in any manner. Thank you, Loeb & Loeb LLP.



August 23, 2022

regulations@coppa.ca.gov

California Privacy Protection Agency

Attn: Brian Soublet

2101 Arena Blvd.,

Sacramento, CA 95834

Re: Comments of Loeb & Loeb LLP in Response to the California Privacy Protection Agency's Notice of Proposed Rulemaking Issued with the Office of Administrative Law on July 8, 2022

The California Privacy Protection Agency (the "Agency") proposed regulations ("Regulations") promulgated pursuant to the California Privacy Rights Act ("CPRA"), which amended the California Consumer Privacy Act of 2018 (collectively with the CPRA, the "CCPA") and is effective January 1, 2023. The California Privacy Protection Agency Board (the "Board") approved the proposed Regulations and the Board filed a Notice of Proposed Rulemaking with the Office of Administrative Law on July 8, 2022.

As a law firm that advises companies of all sizes, across all industry sectors, on how to comply with the CCPA and other privacy laws, Loeb & Loeb LLP ("Loeb") is in a unique position to understand that many businesses who are subject to the CCPA only wish to comply and welcome regulations that help them protect their consumers. We are also in a unique position to offer the Agency insight into some of the practical and technical challenges presented by certain aspects of the Regulations, as well as areas that risk creating confusion, rather than providing clarity. Loeb has multiple offices in California, which means our employees and partners are California residents, in addition to our clients. We have a vested interest in seeing consumers protected in a way that offers further transparency and control over their personal information because we are those consumers.

Loeb has great respect for the task placed before the Agency to promulgate these rules in a way that furthers the privacy of consumers while giving attention to the impact on businesses.¹ That is not an easy balancing act. What we hope to offer in the comments that follow, is some insight into the reality for both businesses and consumers that will help you promulgate rules within that delicate balance. We also hope to respectfully show how portions of the Regulations will only work to confuse and deceive consumers rather than offer further transparency and control over their personal information. We, therefore, submit the following comments in response to the California Privacy Protection Agency's Notice of Proposed Rulemaking issued with the Office of Administrative Law on July 8, 2022.

I. §7001. Definitions.

A. Subsection (h) "Disproportionate Effort"

¹ Cal. Civ. Code §1798.199.40(1).

For purposes of clarity, we offer the following revision to the last sentence in the definition of “disproportionate effort” given other challenges in compliance that might otherwise, independently, rise to the level of disproportionate effort notwithstanding the lack of adequate processes in place:

A business that has failed to put in place adequate processes and procedures to comply with consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer’s request requires disproportionate effort, **unless other evidence of disproportionate effort exists separate and apart from the lack of adequate processes and procedures.**

As an example, a business may have processes in place that the Agency deems inadequate; however, that should not impact the analysis of whether a specific request for information that is maintained in backups or archives for legal or compliance purposes, and is not used for commercial purposes, presents a disproportionate effort. The effort would be disproportionate whether or not the other processes were found to be adequate. We believe this edit creates clarity without diminishing the obligations of any business or the rights provided to any consumer.

B. Subsection(l) “first party”

For purposes of acknowledging situations where more than one business may be consumer-facing and a first party, we propose the following revision to the definition of “first party”:

‘First party’ means the consumer-facing business(s) with which the consumer intends and expects to interact.

As an example, two businesses may co-sponsor an event or a promotion. In these co-branded experiences, it would be clear to the consumer that he or she is interacting with both parties.

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

A. Subsection (a) should remove “unrelated” purposes from the restrictions.

The Regulations provide that if a purpose is “unrelated or incompatible” a business needs explicit consent from the consumer before collecting, using, retaining, and/or sharing the consumer’s personal information.² We propose the removal of “unrelated or” since a purpose could be unrelated but still compatible with the purpose(s) for which the personal information was collected or processed. Further, the CCPA does not prohibit processing for unrelated purposes provided that they are disclosed in compliance with the CCPA and these Regulations once finalized.

As an example, a consumer may register to attend an event and agree to receive emails about other, unrelated events. While these purposes are unrelated, if disclosed, the use of information would be compatible with the consumer’s expectations. Another example is the Agency’s own illustrative example in §7002(b)(2). §7002(b)(2) suggests that internal research and product development is an incompatible purpose, but in fact it is only unrelated. If Business B uses personal information for internal research related purposes that purpose should not be deemed incompatible if disclosed. The purpose of research and development is to create a new product. As an example, consider the number of electronics companies that have created products that are unrelated – you may start with a mobile telephone and expand into VR headsets, fitness watches, and smart home devices. This type of innovation should be encouraged and does

² 11 CCR §7002(a).

not result in a negative impact or harm to the consumer. We should not restrict companies to only the creation of “related” and “expected products.” Particularly where personal information is used internally or shared only with service providers and the use is disclosed, the harm to the consumer is minimal. Requiring additional, explicit consent for purposes that have been disclosed and are not wholly incompatible with the consumer’s expectations (e.g. the example given in 7002(b)(1)) will result in consumers receiving a flood of consent requests for benign activities. Consumers should understand that when they are being asked for explicit consent, that the use case requires their attention and thought before making a decision. These requests should be limited to avoid consent fatigue, which results in consumers consenting to avoid the annoyance of being asked rather than in furtherance of an informed decision.

B. Clarify the conflict in Subsection (a) with the opt-out scheme provided for in the CCPA

The Regulations provide in §7002(a) that businesses must obtain explicit consent from consumers for any purpose that is incompatible with the purpose(s) for which the personal information was collected. However, it is unclear how to reconcile this language with the text of the CCPA, which provides an opt-out (rather than an opt-in) for activities that the Agency may later determine are not compatible with the purpose of collection. As an example, the illustrative examples for when consent is required under §7002(b)(3) and (4) suggest that explicit consent would be needed in circumstances where the text of the CCPA requires businesses to offer an opt-out. If an online retailer gives a delivery company the ability to use the personal information they receive to market another company’s products, that would be a sale and would need to be disclosed to the consumer who could then opt-out of that activity (which would also need to be disclosed under California’s Shine the Light law). Requiring explicit consent in that case is a material change to the text of the CCPA. The Regulations should not require businesses to act in a manner incompatible with the text of the CCPA. Therefore, we propose the following revisions to §7002(a) to offer consumers full transparency into the text of the CCPA and the purposes permitted therein:

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. 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 ~~unexpected or unrelated or~~ incompatible with the purpose(s) for which the personal information is collected or processed. **Notwithstanding the foregoing, where consumers have the right to opt-out of an activity, such opt-out consent shall satisfy the consent obligations described in this Section.**

III. §7003(d). Requirements for Disclosures and Communications to Consumers.

The Regulations provide that for mobile applications, links must be accessible within the mobile application.³ The Regulations also require that the link to the privacy policy be on the platform page or

³ 11 CCR §7003(d). “For mobile applications, a conspicuous link shall be accessible within the application, such as through the application’s settings menu. It shall also be included in the business’s privacy policy, which must be accessible through the mobile application’s platform page or download page.”

download page of the mobile application,⁴ the download or landing page of a mobile application,⁵ and in the application's menu settings.⁶ The notice at collection, may be provided through a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.⁷

We are concerned consumers will be confused and not able to quickly access the links required under the CCPA and the Regulations because the mobile application obligations are inconsistent with the obligations for websites. Consumers are used to finding important information in a drop-down menu within the mobile application because mobile applications have limited space and typically do not have footers and headers like websites. Consumer are hyperaware of this fact. In addition, mobile application providers have no control over the app stores used by consumers to download mobile applications. Taking into consideration the operational complexities with compliance, the current consumer expectation, and the desire to provide consumers with consistent experiences across formats, we offer the following proposed revision to §7003(d):

For mobile applications, a conspicuous link **required under the CCPA or these regulations shall appear in a similar manner as other links used by the business within the mobile application** ~~be accessible within the application~~, such as through the application's settings menu. It shall also be included in the business's privacy policy, which must **also** be accessible through the mobile application's ~~platform page or~~ download page.

The other inconsistent references to the location of required links and notices with respect to mobile applications as we cited to above, should either be removed or revised to align with any changes the Agency chooses to make in response to this comment and/or any similar comments.

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

The Regulations provide:

A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business's intent.⁸

We understand why the Agency is concerned about unintentional dark patterns. After all, regardless of intent, it can still have the effect of substantially interfering with a consumer's choice. That said, outside of the examples provided, there is no definition of a dark pattern in CCPA or the Regulations. Companies should be incentivized to demonstrate a good faith effort to avoid dark patterns, including using an internal review process, engaging in user testing, or employing a similar control. Where those practices have been implemented, and the Agency nevertheless finds that a user interface is a dark pattern, there should be no violation of the CCPA or these Regulations as long as the business promptly takes steps to address the Agency's feedback. We propose the Agency consider the following additional language at the end of §7004(c), in order to take into consideration that many businesses will put forth good faith efforts not to make use of dark patterns and the following will still protect consumers to the fullest extent of the law:

⁴ *Id.*

⁵ 11 CCR §7011(d).

⁶ *Id.*

⁷ 11 CCR §7012(c)(3).

⁸ 11 CCR §7004(c).

The intentional use of a dark pattern shall amount to a violation of the CCPA and these Regulations. An unintentional use of a dark pattern shall not amount to a violation of the CCPA and these Regulations solely to the extent the business can show evidence that the use of the dark pattern was unintentional – for example, by proof that some internal process or review designed to remove dark pattern designs and manipulations was followed prior to implementation) – and the business either (i) stops the processing of personal information for which the dark pattern was the basis of consent for such processing; or (ii) obtains new, valid consent from the consumer to continue such processing.

We believe that this is a good starting point for addressing dark patterns that recognizes the challenges that businesses face, while protecting consumers and incentivizing companies to do the same. Over time, as the definition of dark patterns and the expectations for user interface design become clearer, this position may evolve and the Agency will have an opportunity to be more restrictive in its interpretation of unintentional dark patterns.

V. §7022. Requests to Delete; §7026. Request to Opt-Out; §7027. Requests to Limit.

A. §7022(c) should clarify service providers and contractors responsibility

For purposes of clarity, we ask the Agency to specify in §7022(c) that service providers and contractors that receive a valid deletion request from a business are only obligated to delete the copy of personal information provided by or on behalf of the business to whom the deletion request was submitted. A service provider may have multiple copies of consumers' personal information from multiple clients and it should not be required to delete all records of a consumer's personal information. It should be limited specifically to the business that received the deletion request and subsequently notified the service provider or contractor of the request. Forcing service providers and contractors to delete all records for a consumer could cause the service provider to violate their contract(s) with other clients and removes all consumer choice over the deletion of personal information the service provider or contractor processes on behalf of another business with which the consumer intends to continue to interact.

For example, Business A and Business B each provide Service Provider C with the same copy of Consumer D's personal information. Consumer D wants Business A to delete Consumer D's personal information but wants Business B to continue to process Consumer D's personal information. In order for Business B to continue to provide Consumer D with services, Service Provider C needs to continue processing Consumer D's personal information. If Service Provider C has to delete all copies of Consumer D's personal information, Service Provider C would be in violation of the terms of the contract with Business B and would obliterate Consumer D's choice with respect to Business B. As such, we recommend the following clarification to §7022(c):

A service provider or contractor shall, **solely with respect to personal information received by or on behalf of the business and** upon notification by the business, comply with the consumer's request to delete their personal information by:

B. §7022(e) should clarify record-keeping obligations

The Regulations provide in §7022(e) that:

In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request. The business shall also inform the consumer

that it will maintain a record of the request as required by section 7101, subsection (a). A business, service provider, contractor, or third party *may* retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from its records.

We suggest deleting the last sentence of this section as it conflicts with section 7101(a), which requires that records to be retained for 24 months. As written, it is unclear whether retaining a record of deletion is optional or whether it goes beyond the requirements that are already articulated in §7101(a).

C. Clarifying the disproportionate effort involved in deletion notifications required under § 7022(b)(3)

The Regulations add a new obligation for businesses to notify not only their service providers and contractors of a deletion request, but also the third parties to whom the business sold or shared the personal information. For sales (and now shares), that occur online, there are two general means by which the opt-out is effectuated: (1) the suppression of cookies and other technologies that result in the sale (or share); and (2) passing an opt-out signal. For companies who have built their program and the supporting privacy tech stack to effectuate an opt-out by suppressing the cookies and other technologies that are sales, there is no technical infrastructure to facilitate passing the information about deletion to third parties to whom personal information has been sold/shared. It will require a significant financial and resource investment to build the infrastructure needed to send these notices. The cost will well exceed the \$127.50 projected cost of compliance included in the Agency's economic report. Sending a deletion notice in this case should be deemed a disproportionate effort. There should be no harm to the consumer from this as a consumer that does not want a third party to have their information can exercise their right to opt-out of sale/share.

VI. §7023. Requests to Correct.

A. In §7023(d)(2)(D), Agency should replace “high impact” with “negative impact”

In §7023(d)(2)(D) of the Regulations, a business is to consider the “high impact” on the consumer before asking the consumer for additional documentation to verifying the request to correct and the information to be corrected. It is unclear what a “high impact” would be. For purposes of clarity and consistency, we ask the Agency to instead obligate businesses to assess any “negative impact” on consumers. This gives businesses more direction and aligns directly with the language used in §7023(e).⁹

B. §7023(f)(4) should offer more clarity and consumer transparency

For purposes of clarity and consumer transparency, we propose the following revisions to §7023(f)(4):

If a business denies a consumer's request to correct personal information collected and analyzed concerning a consumer's health, the business shall also inform the consumer that they may provide a written statement to the business to be made part of the consumer's record per Civil Code section 1798.185, subdivision (a)(8)(D). The business shall explain to the consumer that the written statement is limited to 250 words per alleged inaccurate piece of personal information and shall include that the consumer must request that the statement be made part of the consumer's record **and that such statement will be made**

⁹ 11 CCR §7023(e). “A business may delete the contested personal information as an alternative to correcting the information if the deletion of the personal information does not negatively impact the consumer, or the consumer consents to the deletion.”

available to any person with whom it discloses, shares, or sells the personal information collected and analyzed concerning the consumer's health that is the subject of the request. Upon receipt of such a statement, the business shall include it with the consumer's record and make it available to any person with whom it discloses, shares, or sells the personal information collected and analyzed concerning a consumer's health that is the subject of the request to correct.

VII. §7025. Opt-Out Preference Signals.

We propose that the opt-out signal provider be responsible for making it clear to the consumers the opt-out preference signals' limitations. For example, consumers should be informed that the opt-out preference signal (i) is only effective on the browser to which it is downloaded; (ii) it has the effect of helping consumers immediately opt-out of the sale/share of personal information automatically collected by third parties permitted to otherwise collect personal information from the specific website; (iii) anything the consumer directly provides to the business will not be opted out of the sale or sharing; and (iv) more information on how to opt-out of other types of disclosures where permitted by the CCPA can be found in the business's privacy policy. This type of transparency is necessary to prevent consumer deception. It could also harm the relationship businesses, who otherwise operate in good faith to comply with the CCPA, have with these consumers should an opt-out preference signal fail to work as effectively as the opt-out preference signal provider purports and these Regulations purport.

Additionally, for accuracy, and in an effort not to confuse consumers between the letter of the law and rules promulgated by the Agency, we propose the following revision to §7025(e) and (f) respectively:

Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt-out preference signals and providing the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or an alternate opt-out link; or (2) processing opt-out preference signals ~~in a frictionless manner~~ in accordance with these regulations promulgated under Civil Code section 1798.185(a)(19) and not having to provide the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or an alternate opt-out link.

Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by rules promulgated under Civil Code section 1798.185(a)(19) ~~Civil Code section 1798.135, subdivision (b)(1)~~, means that the business shall not..."

VIII. §7026. Requests to Opt-Out of Sale/Share.

The Regulations provide:

A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.

For clarity, we would like the Agency to confirm that a business may use its existing cookie banner or cookie controls to address the opt-out of sale/sharing by updating the user interface of that banner or control

to refer specifically to the right to opt-out of sale/sharing. For many businesses, the only selling/sharing they are participating in is the onward sharing for cross-contextual behavioral advertising. In this case, a cookie banner or similar mechanism may provide the most prominent and familiar means for consumers to opt-out of the sale/sharing of personal information.

IX. §7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.

A. §7027(g)(1) should permit businesses 45 days to comply with requests to limit

The Regulations provide:

A business shall comply with a request to limit by...[c]easing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (l) as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.¹⁰

Sensitive personal information is often manually inputted or uploaded by the consumer, rather than collected through tracking technologies or other automated means. As a result, complying with requests to limit the use and disclosure of sensitive personal information may take more employee resources and effort to effectuate versus a request to opt-out of the sale/share of personal information. The fact requests to limit do not need to be verified does nothing to minimize the amount of time and resources it will likely take to effectuate this right.

As such, we recommend the Regulations provide businesses 45 calendar days to respond to consumer requests to limit, which will put the response time in line with response times for requests to know, delete, and correct.

B. Clarifying §7027(l)

§7027(l) provides:

The purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes ***is not required to post a notice of right to limit.***

This language refers to the requirement to post a notice of the right to limit, but is silent on the obligation to provide two mechanisms to respond to those right. Businesses that only use sensitive personal information for the purposes outlined in subsection (l) should not be required to post a notice of the right to limit or to provide a method to submit a request to limit.

We suggest the following revision:

The purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes ***is not required to post a notice of right to limit or provide a method through which a request to limit may be submitted.***

¹⁰ 11 CCR §7027(g)(1).

X. §7050. Service Providers and Contractors.

A. §7050(c) should account for person(s) who may act as businesses, service providers, contracts, and third parties under one contract because of the multitude of services it provides

The Regulations provide in §7050(c) that “a service provider cannot contract with a business to provide cross-contextual behavioral advertising...A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor.”

We ask the Agency to consider the fact that there are many vendors who act as a business, service provider, contractor, and third party under the same relationship/contract with another business depending on the services being provided to the business. We then ask the Agency to clarify in the Regulations that the above language applies only with respect to the cross-contextual behavioral advertising services:

A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but ~~those services~~ **the service provider** shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or **collects** from its own interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor, **with respect to cross-contextual behavioral advertising services.**

XI. §7053. Contract Requirements for Third Parties.

In §7053(b), the Regulations obligate a business to contractually require third parties that collect personal information from a consumer on its website to check for and comply with a consumer’s opt-out preference signal.¹¹ We ask the Agency to clarify that this satisfies the business obligations with respect to notifying such third parties of opt-out requests for purposes of compliance with §7026(f)(3). To the extent that all sales or shares take place via personal information collected from the website for consumers and a business has required those third parties to check for and honor opt-out preference signals, such third parties will be on notice of any opt-out requests sent via opt-out preference signals. Otherwise, businesses would be required to send a duplicate notice to those third parties.

XII. §7301. Agency Initiated Investigations; § 7302. Probable Cause Proceedings; and §7304. Agency Audits.

¹¹ 11 CCR §7053(b). “A business that authorizes a third party to collect personal information from a consumer through its website either on behalf of the business or for the third party’s own purposes, shall contractually require the third party to check for and comply with a consumer’s opt-out preference signal unless informed by the business that the consumer has consented to the sale or sharing of their personal information.”

We appreciate the importance of the Agency’s ability to audit and enforce the CCPA, but suggest a few protections that would not diminish that ability, but would build in some additional due process and consumer protections.

First, consider including an appeal process for administrative proceedings, especially where the person can offer new additional evidence not previously available to the person.¹²

Second, the Regulations do not appear to protect consumer personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena. The Regulations should include requirements for technical, administrative, and physical safeguards that the Agency must follow in order to protect consumers’ personal information during the performance of the audit and to ensure that the audit is not unduly burdensome. Likewise, information provided in connection with an audit should be protected by a duty of confidentiality. We understand that if a matter escalates, that information may become part of a public record.

Moreover, and pursuant to the CCPA, the Regulations should set forth an objective standard to guide the Agency’s selection of which businesses it will audit, and clarify what constitutes a “significant privacy harm” that could give rise to an audit. Without a clear and objective standard, it will be difficult for businesses to sufficiently cooperate with an audit.

We ask the Agency to be transparent with respect to the steps or procedures it will follow prior to conducting an audit. For example, the Agency should specify with detail the steps it must take before conducting an unannounced audit.

Finally, the Agency should explicitly set out in the Regulations that the Agency is not permitted to conduct audits under the CCPA or these Regulations until the Agency has provided “guidance to businesses regarding their duties and responsibilities under [the CCPA] and appoint[s] a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with [the CCPA] pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185.”¹³

XIII. The Agency Should Delay Enforcement Until After Regulations Are Finalized

While we recognize the Agency was asked to meet an impossible deadline, we ask the Agency to delay enforcement of these Regulations given it has missed the July 1, 2022 deadline to adopt final regulations. Every person subject to the CCPA needs time to implement the Regulations once they are finalized. Our clients ask us on a daily basis how to comply with the CPRA and it has been challenging for use to offer direct and practical guidance on how to comply. Alternatively, we ask the Agency to specify in the Regulations that the Agency will not enforce against violations of the CPRA amendments if such violations occurred prior to July 1, 2023¹⁴; or against violations with respect to obligations only found in proposed regulations; or, with respect to automated decision-making, privacy risk assessments, and cybersecurity audits, until six months after such obligations are addressed in finalized Regulations.

¹² 11 CCR §7302(d). “The Agency’s probable cause determination is final and not subject to appeal.”

¹³ Cal. Civ. Code §1798.199.40(f).

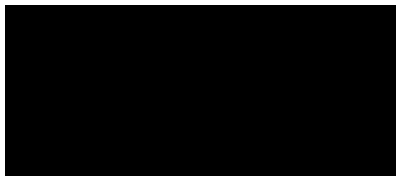
¹⁴ Cal. Civ. Code §1798.185(d). “Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended by this act shall remain in effect and shall be enforceable until the same provisions of this act become enforceable.”

XIV. Conclusion

Again, we want to recognize the task placed before the Agency in promulgating these regulations under the CCPA. We thank the Agency for the immense amount of work it has had to do just to get a draft set of regulations published. We hope that our comments help provide insight into the challenges the Regulations will place on businesses who genuinely want to comply and the potential harm to consumers some of the proposed Regulations may unknowingly cause.

We thank you for your time and consideration.

Sincerely,



Jessica B. Lee
Partner, Chair of Privacy, Security & Data Innovations, Loeb & Loeb LLP

From: **Paul Juncys** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Markus Lampinen** [REDACTED]; **Admin Prifina**
<policy@prifina.com>
Subject: CPPA Public Comment
Date: 23.08.2022 16:48:57 (+02:00)
Attachments: Prifina CPRA comments.pdf (8 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Madam/Sir,

Please find Prifina's comments on the proposed CCPA/CPRA regulations.

Sincerely,

Paul Juncys

--

Paul Juncys, LL.M. (Harvard), Ph.D.
Co-Founder | [Prifina](#)



Comments to the proposed regulations implementing the amendments made by the California Privacy Rights Act (CPRA) to the California Consumer Privacy Act (CCPA).

To

*Office of Science and
Technology Policy (OSTP)*

August 23, 2022

On behalf of

Prifina, Inc.

Address

1250 31st Avenue
San Francisco, CA
94122 USA

Email

policy@prifina.com

To whom it may concern,

Prifina Inc. is a VC-backed data technology company based in San Francisco. We are building a platform that helps individuals collect data from different sources and get everyday value from their data by utilizing applications that run on top of such user-held data. In Prifina's platform, third-party developers can easily build applications and help capture value from data on the user's side.

Prifina would like to applaud the Office of the Attorney General (OAG) and the California Privacy Protection Agency (CPPA) for their continuous efforts in building stronger foundations for the protection of personal data of individual consumers and setting the framework for how companies access and utilize user-generated data. CPRA and accompanying regulations will be a significant contribution to this domain.

The attached document contains several comments and recommendations on modifying and improving the proposed CPRA regulations. We also offer additional insights about the possible legal and regulatory aspects related to the newly emerging approaches to data (namely, the user-held data model). We would like to invite the staff members of the OAG and the CPPA to explore this new approach to data which we believe could pave the way for designing a more user-centric data ecosystem. The user-held data model offers numerous opportunities for large enterprises, developers, and individual consumers and helps unlock value from user-generated data. We hope that our insights and recommendations will help the OAG and CPPA consider various alternatives in making data compliance processes more efficient, transparent, and fair to various stakeholders in the market.

Should you have any questions, please do not hesitate to contact us.

Sincerely yours,

Markus Lampinen, Jouko Ahvenainen and Paul Jurcys

Prifina's Comments on the Proposed Regulations Implementing the California Privacy Rights Act (CPRA)

August 23, 2022

Initial Observations

The Prifina team applauds the Office of the Attorney General (OAG) and the California Privacy Protection Agency (CPPA) and the incredible work that is being done in positioning California as a blueprint for data privacy protections in the US and beyond. The proposed CCPA/CPRA regulations are a significant step forward. The proposed regulations remarkably improve the implementation of the principles of data minimization and purpose limitation, correctly identify and address problems that consumers face when dealing with dark patterns and deceptive design and rightfully extend the application of data privacy protections to downstream third parties and service providers with whom businesses will be required to enter into privacy-preserving contractual relationships.

We also welcome the innovative approach adopted in the proposed CCPA/CPRA regulations whereby certain rules contain numerous illustrations of their practical application. At the same time, we would like to draw the attention of the OAG and CPPA that underlying technologies related to data privacy compliance, data processing and data architecture are evolving quickly. One particular area of development related to wearable and IoT devices that are becoming available to consumers at increasingly lower prices. Therefore, we would like to suggest reviewing the "classical" examples provided in the proposed CCPA/CPRA regulations and include illustrations from consumer health and wellness wearables and other IoT devices.

Previously, the Prifina team has submitted comments to the earlier drafts of the draft CCPA regulations, and we have also published an overview of the 250+ stakeholder comments to the proposed CCPA Regulations.¹

Definitions: “Average Consumer”

The proposed regulations introduce a concept of an average consumer which is not defined in section 7001. In particular, the term “average consumer” is referred to in section 7002(b) (Restrictions on the Collection and Use of PI), section 7027(a) and 7027(l) (Requests to Limit Use and Disclosure of Sensitive PI), and section 7053 (a) (Contract Requirements for Third Parties). From the business perspective, it would be desirable if the CPPA could provide some guidance on the meaning of “average consumer” because it would help businesses determine the necessary standard of care. In doing so, the CPPA should explain the relationship between “average” and “rational” consumers. Furthermore, we would like to note that depending on the nature of the interaction between a business and consumers, there can be different dimensions of “average”:

- ***Sophistication***: in some interactions, businesses may interact with highly sophisticated “average” consumers (e.g., complex interactions requiring specific knowledge which is well above of an “average” individuals assumed knowledge);
- ***Commercial vs. non-commercial settings***: in some instances, businesses may interact with consumers who may also be businesses (e.g., SAAS services between two business entities);

¹ The study of stakeholder comments to the proposed CCPA regulations - “Principles of Data Privacy in California: Study of Industry Reactions and Comments to the Proposed CCPA Regulations and User-Centric Perspectives” - is available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3601948

- ***Technical knowledge:*** businesses may have consumers who possess more deep technical knowledge about the operation of certain technologies (e.g., software developers);
- ***Expectations of consumers:*** it is possible to differentiate consumers into different groups based on their expectations about how a business accesses, collects and uses consumer data;
- ***Types of data involved:*** the notion of an “average” consumer may depend on how savvy consumers are in understanding the value of their personal data. More specifically, in the past years, we have seen the proliferation of health and wellness wearable devices that help individuals track and get close insights into their health and wellness data. It is possible, that consumers who have one or more health or wellness wearable device are likely to have a greater understanding of their own health and wellness data; and the “average” consumer who owns a smart health and wellness device is more data-savvy than an “average” consumer who has no wearable devices.

The bottom line here is that there is no one-size-fits-all definition of an “average consumer.” Rather, we would like to suggest clarifying that the notion of an “average consumer” should be functional and understanding in a specific type of interaction between a business and a consumer.

Requests to Know (S. 7024)

Section 7024 of the proposed regulations establishes the main principles for how businesses should comply with the consumers’ requests to access the data that businesses have collected about consumers (“requests to know”). Section 7024(k) of the proposed regulations specifies certain categories of data that businesses are required to disclose to the individual consumers (e.g., categories of PI collected in the

preceding 12 months, categories of sources, categories of third parties with whom the business is sharing and selling PI, etc.).

We would like to draw the attention of the OAG and CPPA to the fact that since the adoption of the CCPA and accompanying regulations, there has been a remarkable progression in terms of what data can be accessed by consumers. More specifically, both regulators in other jurisdictions (such as the EU), as well as various market stakeholders, are exploring ways to unlock the data from silos and allow consumers request access to virtually all user-generated data. The most remarkable example in this regard is the proposed European Data Act. In the same vein, we at Prifina, believe much value could be created if consumers were able to access greater amounts of data (not just input data).² The same trend to give consumers access to more user-generated data observed in the data market as well. There are moral and utilitarian reasons why consumers should be able to access the data they generate while utilizing various online services and hardware devices.

Yet, Section 7024 of the proposed CCPA/CPRA regulations still refers to “categories” of data. Therefore, we would like to encourage the OAG and CPPA to update section 7024(k) of the proposed regulations and expand the scope of the data that consumers can access from businesses.

Prifina’s User-held Data Model

Prifina is a VC-backed company building a new data architecture where individuals own and control their data ("user-held data model"). This type of data architecture enables new use cases and personal applications to be designed and built on top of user-held data.

² For a more detailed discussion, see Paulius Jurcys and Markus Lampinen, “Prifina Comments on the Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)” available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4110462 and Paulius Jurcys, “The Proposed EU Data Act: 10 Key Takeaways” available at: <https://medium.com/prifina/the-proposed-eu-data-act-10-key-takeaways-6a380303c4f0>

Prifina's mission is to create an environment where individual users can get daily value from their personal data and where developers can build applications that help generate value from such user-generated and user-held data. We believe that personal and user-generated data can help individuals improve the quality of their lives and that personal data has long-term value to individuals.

The starting premise of Prifina's user-held data model is the ability of each individual to collect their data from various data sources (wearable devices such as smartwatches or smart rings, online accounts, paper documents, etc.) into their "personal data clouds." Every personal data cloud is supported by a dynamic software layer that cleans and organizes the data format and makes data efficiently utilizable by apps. By default, only the user can access data in the personal data cloud; third parties cannot access any data unless the user gives prior express authorization. Prifina's user-held data model is user-centric: the user has exclusive and ultimate agency and control over the data held in the personal data cloud. Furthermore, in the user-held data environment, individuals can be considered to be legal owners of their user-held data (i.e., the data in each user's personal data cloud).

The "user-held data model" opens new opportunities for generating value from personal and user-generated data. Prifina is developing an intelligent data layer that helps normalize the data that is collected in users' personal data clouds. Using Prifina's resources and tools, developers can easily add new data sources and build new applications that run on top of user-held data (i.e., apps run locally in each user's personal data cloud). As a result, the value from user-held data is captured on the user's side.

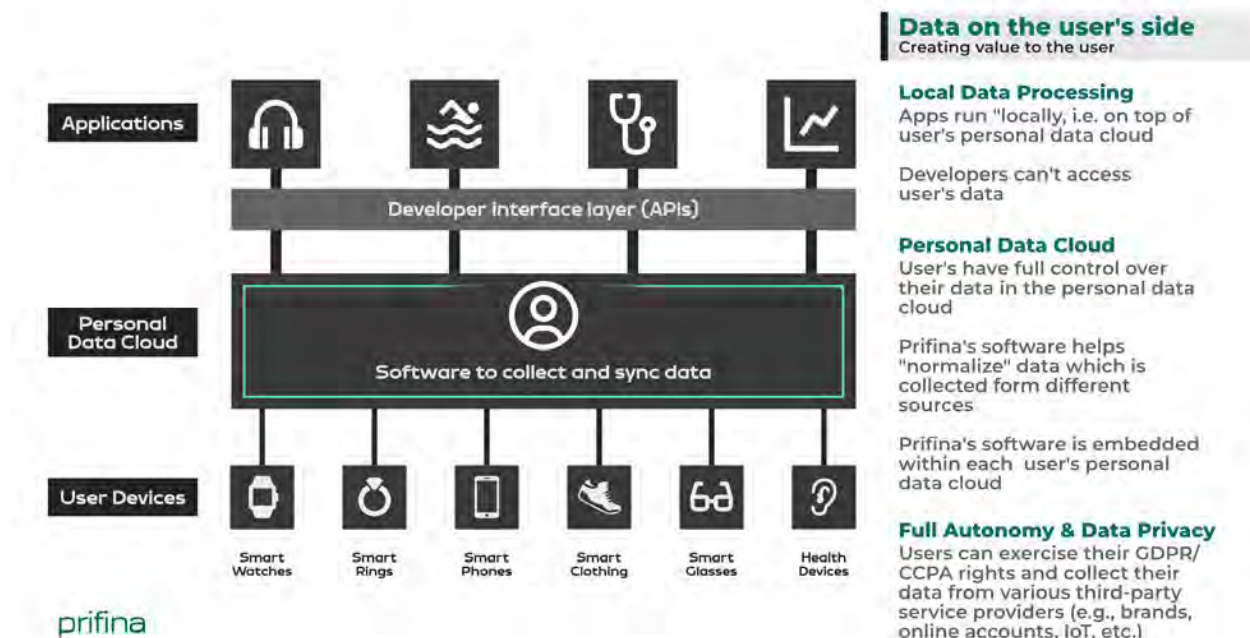
The user-held data model has two important implications: First, users can better understand the depth and breadth of their data and have full ownership and control over it. Secondly, the user-held data model separates data from the applications.

This user-centric, user-held data approach is in line with the general principles of data privacy laws: that data is being used only with the user's prior consent, data minimization (here, the service provider does not have to hold any data on its own

servers), transparency, purpose limitation (that data is used only for clearly defined purpose), data security, data portability, and even cross-border data transfers.

The user-held data model opens new perspectives concerning the portability of personal and user-generated data. Rather than data being "ported" from service provider A to service providers B and C, service providers come to every user through new applications that run in users' personal data clouds. This means that service providers can better understand their potential customers by offering apps that run in the consumer's local environment. This kind of new architecture where data is "activated" and processed on the user's side enables businesses to avoid huge risks associated with holding customer data on their own servers.

The user-held data model offers compelling technological architecture and multi-stakeholder incentives to build a new data ecosystem based on human-centric data values. This data model inspires people to think about "activating" data to unlock the value from data for individuals and developers/businesses and open the gates to building user-centric data apps for "smart citizens." Furthermore, the user-centric data model will likely become one of the possible technological solutions for utilizing user-generated data for research and reaching sustainability goals.



Further references:

- P. Jurcys, M. Corrales Campagnucci, and M. Fenwick, "The future of international data transfers: Managing legal risk with a 'user-held' data model", Computer Law & Security Review, Vol. 46 (September 2022), available at: <https://www.sciencedirect.com/science/article/abs/pii/S0267364922000383>
- P. Jurcys et al. "Ownership of User-Held Data: Why Property Law is the Right Approach", Harvard Journal of Law and Technology Digest (September 2021) available at: <https://jolt.law.harvard.edu/digest/ownership-of-user-held-data-why-property-law-is-the-right-approach>

From: **Snell, James (Jim) (PAO)** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CCPA Public Comment
Date: 23.08.2022 23:50:15 (+02:00)
Attachments: 2022-08-23 Client CPRA Regulation Comments.pdf (11 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please find attached a client's CPRA comments. We appreciate the opportunity the Agency has provided for comments. Best,

James (Jim) Snell | Perkins Coie LLP

PARTNER

3150 Porter Drive

Palo Alto, CA 94304-1212

M. [REDACTED]

D. [REDACTED]

F. [REDACTED]

E. [REDACTED]



Perkins Coie is ranked Band 1 in Privacy & Data Security: Litigation by Chambers USA.

Ranked among the best in the nation for Privacy & Data Security Law by Chambers USA.

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.



3150 Porter Drive
Palo Alto, CA 94304-1212

+1.650.838.4300
+1.650.838.4350
PerkinsCoie.com

August 23, 2022

James G. Snell

D. [REDACTED]
F. [REDACTED]

BY E-MAIL

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834
regulations@coppa.ca.gov

Re: Comments on Agency's First Draft of Proposed CPRA Regulations

Dear Mr. Soublet:

Please find below comments on behalf of an anonymous client to the California Privacy Protection Agency's ("Agency's") proposed regulations implementing the California Privacy Rights Act ("CPRA"). To be clear, these comments are not provided on behalf of Perkins Coie LLP, and do not necessarily reflect the views of Perkins Coie LLP, but instead reflect comments from a client who asked that we submit such comments on their behalf. We thank the Agency for considering these comments and look forward to the opportunity to comment on future rulemaking efforts.

1. Introduction and General Considerations

My prior comments on behalf of this client with respect to the September 22, 2021, Invitation for Preliminary Comments on Proposed Rulemaking Under the CPRA, dated November 8, 2021, prioritized two overarching principles for the Agency to consider: (1) seek to align the Regulations with other similar privacy laws to promote privacy-preserving business practices and consumer understanding and (2) allow businesses flexibility in meeting their compliance obligations under the law. Although the proposed regulations reflect these principles in many areas, areas remain where the proposed regulations could be honed further and enhanced to better achieve such critical goals. Accordingly, we offer the below general recommendations for the Agency's consideration, and we follow with comments on particular provisions in detail below.

To the greatest extent possible, seek to harmonize the CPRA and the final regulations with existing privacy regimes and other similar privacy laws to promote consumer understanding and support development of privacy-preserving business practices. The CPRA provides that, "[t]o the extent it advances consumer

Brian Soublet
 August 23, 2022
 Page 2

privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions.”¹ Moreover, the CPRA states that the Agency shall “[c]ooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.”² The proposed regulations can and should be further aligned with existing privacy regimes and with other states’ new omnibus consumer privacy laws. As currently drafted, the proposed regulations would force companies to adopt California-specific user choices, contracts, and notices while adopting different choices, contracts, and notices to comply with other states’ laws. Even apart from the ensuing compliance costs, this lack of harmonization would confuse consumers’ understanding of their rights and impede companies’ development of privacy-preserving data practices.

Rather than create new and onerous obligations, prioritize compliance with the existing provisions in the CPRA. Contrary to the CPRA’s purpose of strengthening consumer privacy “while giving attention to the impact on business and innovation,” the proposed regulations add new and highly prescriptive requirements.³ The CPRA’s goals would be better achieved via more flexible standards that focus on compliance with the existing requirements rather than adding requirements that put form over substance. For example, the proposed regulations add to already highly prescriptive and arduous requirements for contracts with service providers⁴ and notices at collection,⁵ and also add entirely new and onerous requirements for contracts with third parties, while providing that any failure in form to meet these standards could result in material violations of the law and substantial fines, irrespective of whether consumers are in fact confused, much less harmed, by such divergence from the prescribed form. For instance, the proposed regulations could deem businesses to be “selling” personal information simply by providing it to a service provider where the governing paper of such transfer fails to fully address one of the ten required elements for such contracts (regardless of whether the service provider is substantively compliant under the law).⁶ Similarly, the dark patterns requirements in large part could impose violations even where there is not a substantial impact on consumers or any consumer confusion.⁷

Such prescriptive obligations would divert scarce compliance resources to highly technical and formalistic privacy programs. Thus, we recommend that the Agency reconsider its highly detailed and prescriptive approach, favoring flexible rules, or, at least, rules clarifying that only a *material* failure to abide by the regulations would be considered a violation of the law.

¹ CPRA § 3(C)(8).

² *Id.* § 1798.199.40(i).

³ *Id.* § 3(C)(1).

⁴ *See, e.g.*, Proposed Regulations § 7051.

⁵ *See, e.g., id.* § 7012(f).

⁶ *See generally, id.* § 7051(c).

⁷ *Id.* § 7004(b) (stating that any user interface that fails to meet the highly detailed requirements of the proposed regulations “may be considered a dark pattern”).

Brian Soublet
 August 23, 2022
 Page 3

2. Restrictions on the Collection and Use of Personal Information (Sec. 7002)

Under the CPRA, permitted processing purposes are those “reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected.”⁸ The proposed regulations would depart from the text of the law, creating a standard for what is “reasonably necessary and proportionate” that is based on a new concept of what is either “consistent with what an average consumer would expect” at the time of collection, or what would be “compatible with what is reasonably expected by the average consumer.”⁹

This new standard is not only confusing and operationally challenging, but also would arguably prohibit businesses from processing for properly disclosed and legally compatible uses. For instance, there may be uses that an average consumer might not expect (*e.g.*, innovation, fraud prevention, etc.) that would be entirely compatible with the context in which the personal information was collected. These uses would not harm consumers (indeed, they would benefit from them). Such a result not only contravenes the CPRA’s text, but is also incompatible with laws in other jurisdictions and longstanding privacy principles, which recognize the role of consumer disclosures in determining the scope of permitted processing.¹⁰ Section 7002(a)’s “average consumer expectation” standard, interpreted broadly, could threaten to stifle even key data uses such as for providing and improving consumer services, driving companies to ponder whether such processing would be expected by an “average” consumer. This would potentially and materially inhibit innovation, and arguably deprive consumers of the use of their personal information for developing new services, even in privacy-preserving ways. Such a standard would also risk conflicting with other privacy laws, both in the U.S. and globally, which, like the CPRA itself, focus on limiting processing to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer.¹¹

⁸ CPRA § 1798.100(c).

⁹ Proposed Regulations § 7002(a).

¹⁰ See, *e.g.*, *The Fair Information Practice Principles*, Int’l. Ass. of Privacy Professionals, <https://iapp.org/resources/article/fair-information-practices/> (last visited Aug. 23, 2022) (explaining that a company’s specification of their use of personal information prior collection is a principle of fair information use); See also, *Privacy Online: Fair Information Practices In the Electronic Marketplace*, Fed. Trade Comm., <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf> (discussing that, for the past thirty years, notice of how information is used has been a key principle for determining if an information practice is fair).

¹¹ See General Data Protection Regulation (“GDPR”) Art. 5; Colo. Rev. Stat. § 6-1-1308(3); Connecticut Data Privacy Act (“CTDPA”), S.B. 6, 2022 Gen. Assemb., Reg. Sess. (Conn. 2022) § 6(a); VA. Code Ann. § 59.1-574.A.

Brian Soublet
 August 23, 2022
 Page 4

Determining whether processing is “reasonably necessary and proportionate” or “compatible with the context in which the personal information was collected” should not be based on the supposed expectations of “average” consumers. Consumers, for example, may lack an understanding of how data is collected, used, and disclosed to protect against important considerations like meaningful product improvement, or privacy enhancing services like minimizing fraud. Similarly, the examples provided in Section 7002(b) should emphasize the statutory standard of compatible processing purposes rather than introduce new and subjective concepts such as “unexpected” or “unrelated” data use, which would invite unnecessary confusion especially when compared to laws of other jurisdictions. For instance, while product improvements may generally be viewed as “compatible” uses, they may be claimed to be “unexpected” by a consumer.

We suggest that the Agency revert to the language of the CPRA. Failing that, we suggest that the Agency revise the proposed regulations such that they (1) implement better understood notions of “reasonable” consumers rather than “average” ones, and (2) clarify that consumer-facing notices inform the expectations of reasonable consumers. Also, absent reference to disclosed uses in the examples in Section 7002(b), they risk interrupting fully disclosed and privacy-sensitive uses of personal information.

Proposed Amendments:

Sec. 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.~~ 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 ~~was not disclosed when the personal information was collected or is otherwise unrelated or~~ incompatible with the purpose(s) for which the personal information was collected or processed.”

We also suggest that the examples listed in Section 7002(b), remove the term “average” and replace it with “reasonable” and also delete the phrase “unrelated to” or replace it with the phrase “incompatible with.”

Brian Soublet
 August 23, 2022
 Page 5

3. Working With Service Providers, Contractors, and Third Parties (Sec. 7051 and 7053)

A. Requirements for Agreements with Service Providers, Contractors, and Third Parties (Sec. 7051(a)-(d) and 7053)

The proposed regulations would impose new, substantive requirements for agreements with service providers, contractors, and third parties, beyond those imposed by the CPRA. And failure to include any of the ten requirements for contracts with service providers/contractors or the six requirements for third party contracts could be deemed a violation, potentially exposing businesses to significant penalties even for immaterial non-compliance with any aspect of the contract provisions (regardless of whether the party was abiding by the CCPA).¹² These detailed requirements, coupled with stringent consequences for immaterial non-compliance, would impose substantial compliance costs on companies' practices with minimal, if any, corresponding benefit to consumers. For example, requiring companies that "sell" or "share" personal information to third parties to document the specific purposes of such disclosures or permitted uses is overly burdensome given that the recipient company often has the right to use the information received broadly consistent with the law.

If the Agency does not remove the additional prescriptive requirements for contracts with service providers, contractors, and third parties, it should add a materiality standard such that companies would not be punished for trivial violations or immaterial non-compliance.

Proposed Amendments:

We propose that the Agency strike Section 7051(a)-(d). Alternatively, we propose that the Agency edit Section 7051(c) as follows:

Sec. 7051(c): "A person who does not have a contract that complies **in material respects** 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 **in material respects** 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."

B. Businesses' Required Due Diligence of Service Providers and Contractors (Sec. 7051 (e))

¹² Proposed Regulations § 7053(c).

Brian Soublet
 August 23, 2022
 Page 6

In addition to the numerous substantive requirements for contracts with service providers and contractors, the proposed regulations would impose potential liability on businesses for the acts of the counterparties with whom they contract. In particular, under the proposed regulations, businesses could be deemed to have knowingly provided personal information to a service provider who intended to use it in violation of the law, simply by providing the information to a service provider without having tested such provider's systems. In essence, this provision unduly exposes businesses to potential liability for the acts of the service provider with whom they contract (even where the business is substantively in full compliance with the CCPA). This provision would also supplant the CPRA's actual knowledge/reason to believe standard at Section 1798.145(i).¹³ Accordingly, we recommend striking Section 7051(e) in its entirety.

Proposed Amendment:

Sec. 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 nor exercises its rights to 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.”~~

4. Agency Audits (Sec. 7304)

In earlier comments, we suggested that the Agency should confirm that Agency audits take place only where there is a credible claim that the business has violated a substantive provision of the CPRA that creates a risk of harm to consumers. We also recommended that the scope of audits should be limited to the provision(s) alleged to have been violated by the business. Anchoring audits in this manner would maximize the Agency's effectiveness of audits that benefit consumers while also minimizing the compliance burden on businesses. We also recommended that the Agency confirm that audits are confidential and are not required to be made public, and that adequate protections should also be recognized for privileged and confidential information, including trade secrets and other proprietary and confidential information, as well as consumers' personal information.

¹³ See CPRA § 1798.145(i) (“A business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider or contractor intends to commit such a violation.”).

Brian Soublet
 August 23, 2022
 Page 7

While we recognize the Agency's key role in ensuring CCPA compliance, the proposed regulations would compel companies to undergo "unannounced" audits without specified procedures or processes for how these audits are to be conducted. Again, we respectfully request that the Agency include regulations that address the above concerns.

In addition to the above concerns, while the CPRA limits¹⁴ the Agency's audit authority to "*businesses*," the proposed regulations would permit the Agency to audit "business[es], service provider[s], contractor[s], or person[s]." The Agency should clarify that, consistent with the CPRA, only businesses are subject to Agency audits.

Further, the use of "unannounced" audits threatens due process and is likely to be both resource intensive and an inefficient allocation of limited Agency resources given that businesses would be ill-prepared to address audit inquiries. "Unannounced" audits could also unduly threaten personal, privileged, and confidential information. The current proposed provisions could better balance these important considerations and build in important due process protections. We suggest that the Agency should be required to provide at least 30 days' notice prior to forcing businesses to undergo an audit.

The regulations should provide certain reasonable limitations on the circumstances under which the Agency may conduct audits and the processes by which they do so. For instance, the Agency should only be permitted to conduct audits where the Chief Privacy Auditor has a reasonable suspicion of an ongoing CCPA violation, and only with respect to the scope of that suspected violation. In addition, audits should be limited to Agency review of existing records, books, or papers. They should also be limited in time. The audit notice should state the provision of the CCPA which serves as the basis for the audit; describe the suspected violation; identify the records, books, or papers intended for Agency review; and provide the date and time of the audit. Such safeguards would preserve important due process rights, and enable more cost-effective audits, thereby conserving the Agency's finite resources. Relatedly, the Agency should provide further basis and process for the procedures proposed for failures to cooperate.

Finally, the CPRA tasks the Agency with issuing regulations to "protect consumers' personal information from disclosure to an auditor, in the absence of a court order, warrant, or subpoena."¹⁵ We respectfully request that more be done to ensure that consumers' personal information is protected through the course of an Agency audit.

¹⁴ See CPRA § 1798.199.10(f) ("Members of the Agency board shall . . . appoint a Chief Privacy Auditor to conduct audits of *businesses* to ensure compliance with this title pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185") (emphasis added); *id.* § 1798.199.65 (referring to the Agency's "power to audit a *business's* compliance with this title") (emphasis added).

¹⁵ See CPRA § 1798.185(a)(18).

Brian Soublet
 August 23, 2022
 Page 8

Proposed Amendments:

Sec. 7304: “(a) Scope. The Agency may audit a business’s existing books, papers, or records, ~~service provider, contractor, or person~~ to ensure compliance with any provision of the CCPA. The scope of the audit shall be limited to the CCPA provision that the Agency reasonably suspects is being violated, and shall be limited to a time frame reasonably necessary to audit the suspected violation.

(b) Criteria for Selection. The Agency may conduct an audit ~~to investigate possible violations of where the Chief Privacy Officer finds reasonable suspicion that a business is violating a provision of the CCPA. Alternatively, the Agency may conduct an audit if the subject’s collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.~~

(c) Audits must be announced ~~to the business or unannounced as determined~~ by the Agency in writing with thirty days’ notice. Such notice shall identify the provision of the CCPA that serves as the basis for the audit; describe the suspected violation; identify the books, papers, or records the Agency intends to review; and provide the date and time of the audit.

(d) Failure to Cooperate. A subject’s failure to cooperate during the Agency’s audit may result in the Agency issuing a subpoena ~~for the books, papers, or records at issue, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.~~

(e) Protection of Personal Information. ~~The Agency shall not seek disclosure of consumer personal information during an audit in the absence of a court order, warrant or subpoena. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977, Civil Code section 1798, et seq. Audits shall be confidential. At the conclusion of the audit, the audited party may request the destruction or return of any materials provided by the audited party.”~~

5. Enforcement (Sec. 7301 - 7303)

A. Agency-Initiated Investigations (Sec. 7301)

The CPRA allows the Agency to investigate “possible violations” of the law.¹⁶ In initiating investigations, the Agency should, at minimum, be required to have a reasonable suspicion that a business has violated the

¹⁶ CPRA § 1798.199.45.

Brian Soublet
 August 23, 2022
 Page 9

law. This would better align the draft regulations with the language of the CPRA. Such a limit would also conserve Agency resources, allowing it to better focus on instances where a violation may exist. Further, this would benefit businesses by ensuring that investigations are not initiated where there is no reasonable suspicion of a violation.

Proposed Amendment:

Sec. 7301: “All matters that do not result from a sworn complaint, including Agency-initiated investigations, referrals from government agencies or private organizations, and nonsworn or anonymous complaints, may be opened on the Agency’s initiative, **but only where the Board, by a majority vote, finds reasonable suspicion that a business has violated the CCPA.**”

B. Probable Cause Proceedings (Sec. 7302)

Under Section 7302, probable cause proceedings “may be conducted in whole or in part by telephone or videoconference,” if the proceeding is “not open to the public.”¹⁷ But the CPRA provides persons alleged to have violated the CPRA the right to be “present in person” at any proceeding of the Agency.¹⁸ The Agency should clarify that businesses have the right to a live proceeding upon request, even in the case of private proceedings. Moreover, the proposed regulations should clarify that the Agency’s probable cause determination as a result of such proceeding is not final in the sense that it serves as a binding finding or ruling; rather, such determination should only be final for the purpose of the Agency holding an administrative hearing to determine whether there has been a violation of the CCPA under Cal. Civ. Code § 1798.199.55.

Proposed Amendments:

Sec. 7302: “(b) Probable Cause Notice. The Enforcement Division will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50. **Such notice shall contain a clear statement of each claim against the alleged violator and a summary of the evidence in support of each such claim, as well as the documents and other evidence on which the Enforcement Division Staff will rely at the proceeding.**”

¹⁷ Proposed Regulations § 7302(c)(1).

¹⁸ See CPRA § 1798.199.50 (“No finding of probable cause to believe this title has been violated shall be made by the Agency unless, at least 30 days prior to the Agency’s consideration of the alleged violation, the business, service provider, contractor, or person alleged to have violated this title is notified of the violation by service of process or registered mail with return receipt requested, provided with a summary of the evidence, and informed of their right to be present in person and represented by counsel at any proceeding of the Agency held for the purpose of considering whether probable cause exists for believing the person violated this title.”).

Brian Soublet
 August 23, 2022
 Page 10

(c) Probable Cause Proceeding. (1) The proceeding shall be closed to the public unless the alleged violator files, at least 10 business days before the proceeding, a written request for a public proceeding. If the proceeding is not open to the public, then the proceeding, **at the election of the alleged violator**, may be conducted in whole or in part by telephone or videoconference. . .

(d) Probable Cause Determination. Agency staff shall issue a written decision with their probable cause determination and serve it on the alleged violator electronically or by mail. The Agency's probable cause determination is final **for the purpose of determining that the Agency may hold an administrative hearing to determine whether there has been a violation of the CCPA under Cal. Civ. Code § 1798.199.55** and not subject to appeal. **If probable cause is not found, the Agency shall, at the alleged violator's request, destroy or return any materials provided by the alleged violator.**

(e) Unless the probable cause proceeding is open to the public at the request of the alleged violator, notices of probable cause, **information or arguments presented at the probable cause proceeding by the parties**, and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA."

6. Technical Specifications for Opt-Out Preference Signals (Sec. 7025(b))

The CCPA requires the Agency to "issue regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information."¹⁹ The law further outlines the topics that the regulations must address, including how the choice must be presented, such as to ensure that the opt-out preference signal is consumer-friendly, clearly represents a consumer's intent, and does not conflict with other settings.²⁰

The Agency has not yet followed the specifications in the CPRA through the proposed regulations' current form, instead requiring companies to honor any opt-out preference signal that "is in a format commonly used and recognized by businesses" such as an HTTP header field²¹ and providing that 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"²² and need not be tailored only to California or to refer to California. We urge the Agency to fulfill its statutory obligation to

¹⁹ See CPRA § 1798.185(a)(19).

²⁰ See *id.*

²¹ Proposed Regulations § 7025(b)(1).

²² See *id.*

Brian Soublet
August 23, 2022
Page 11

provide clear guidance regarding opt-out signals in a way that makes it possible for companies to honor these signals and to build meaningful compliance programs.

Proposed Amendment:

We propose that the Agency strike Section 7025 of the proposed regulations in its entirety until the Agency defines the requirements and technical specifications for opt-out preference signals.

* * * * *

We appreciate the Agency's hard work on the CPRA regulations and we appreciate the opportunity to provide comments on the proposed regulations.

Sincerely,



James G. Snell

From: **Alexander Bennett** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: Privacy Regulations Comments
Date: 23.08.2022 19:53:11 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear California Privacy Protection Agency,

I have the following recommendations to improve the regulations:

(1) Section 7002: provide new examples

The restrictions on the collection and use of personal information include "Illustrative Examples" that are clearly previous FTC cases: Goldenshores and Everalbum. This could cause confusion because the FTC took action in these cases on the basis of its authority over unfair and deceptive commercial acts and practices. The Agency is implicitly citing these cases in support of a different legal standard - uses that are "[in]compatible with what is reasonably expected by the average consumer." Given the potential to confuse people about the applicable legal standard, the Agency should provide original illustrative examples.

(2) Section 7015: remove the "Icon" requirement for alternative optout links

The "Opt-Out Icon" is confusing and clashes with many website themes. There is a reason it has seen virtually zero adoption by websites governed by CCPA.

Businesses should be encouraged to make exercising rights easier without having to jump through a series of hoops. Controls like the alternative opt-out link that enable users to exercise multiple rights at once should be encouraged. However, requiring that businesses who provide the alternative opt-out link must display the "Opt-Out Icon" will disincentive them from providing this link in the first place. Therefore, the requirement to show the icon should be deleted.

(3) Section 2027: Issue regulations on sensitive personal information that does not infer characteristics

The CPRA creates a new right to restrict use and disclosure of sensitive personal information. However, it also provides that this right does not apply to all sensitive personal information, only information that is collected or processed for the purposes of "inferring characteristics about a consumer." Unfortunately, this carveout is not addressed in the regulations and might confuse people into thinking that all sensitive personal data is subject to this right. Therefore, clarification is necessary.

Thank you.
Alex

From: **Twilla Case** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 16:53:43 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

All consent should be explicit opt-in. This is the only way consumers will truly know who has their data.

Explicit opt-in will dramatically decrease the amount of data companies have on us. Due to less data being kept, the cost of notifications and security will decrease as well.

There should be a LOT more education, using layperson's terms, to the general public about data privacy.

There needs to be a tremendous uptick in enforcement actions.

Please do not allow the ADPP to dilute Californian's privacy.

Twilla Case
[REDACTED]

Sent from my iPhone

From: **Lusine Chinkezan** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Kyla Christoffersen Powell** [REDACTED]
Subject: CPPA Public Comment
Date: 23.08.2022 23:56:19 (+02:00)
Attachments: CJAC Comments CPPA Rulemaking 8-23-22.pdf (19 pages)
WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

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

Dear CPPA:

The Civil Justice Association of California hereby submits its comments on the CPPA's proposed regulations implementing the Consumer Privacy Rights Act of 2020.

[Lusine Chinkezan](#)

Counsel

Mobile [REDACTED] | www.cjac.org





August 23, 2022

Sent via email

California Privacy Protection Agency
Attn: Brian Soublet
regulations@coppa.ca.gov

Re: *Comments by the Civil Justice Association of California on Proposed Rulemaking Under the California Privacy Rights Act of 2020*

Dear California Privacy Protection Agency Board and Staff:

The Civil Justice Association of California (CJAC) appreciates the opportunity to provide comments on behalf of our member companies and organizations to the California Privacy Protection Agency ("Agency") proposed regulations under the California Consumer Privacy Act (CCPA), as modified by the California Privacy Rights Act of 2020 (CPRA).¹

By way of context for our below comments, our members and other businesses attempting to comply with, first the CCPA, and now the combined CCPA and CPRA, have found implementation to be challenging from the start. The frequent changes to the statute and rules have compounded the difficulty of understanding and implementing their complex and expansive provisions.

Over the course of many comment periods and public hearings, CJAC and numerous others have urged policymakers and regulators to provide clarifications and revisions to make implementation and compliance feasible for businesses, while still meeting the consumer protection goals of the statute. This balancing is captured in CPRA's rulemaking instructions:

[The Agency] shall solicit broad public participation and adopt regulations to further the purposes of this title, including but not limited to, the following areas:

- (a)(19)(C) Issuing regulations, ***with the goal of strengthening consumer privacy, while considering the legitimate operational interests of business***, to govern the use or disclosure of a consumer's sensitive personal information, notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information, including:
 - (i) determining any additional purposes for which a business may use or disclose a consumer's sensitive personal information;
 - (ii) determining the scope of activities permitted under paragraph (8) of subdivision (e) of section 1798.140, as authorized by subdivision (a) of

¹ CJAC is a more than 40-year old nonpartisan, nonprofit advocacy organization representing a broad and diverse array of businesses and trade associations. A trusted source of expertise, we confront legislation, laws, and regulations that create unfair litigation burdens on California businesses, employees, and communities. Toward that end, CJAC offers research and guidance on policy issues that impact civil liability.

Section 1798.121, to ensure that the activities do not involve health-related research;

(iii) ensuring the functionality of the business's operations; and

(iv) ensuring that the exemption in subdivision (d) of section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer, while ensuring that businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information under section 1798.121.²

We commend the Agency board and staff for their significant accomplishment of issuing the pending extensive proposed rulemaking as quickly as you have, given the short timeframe provided to the Agency for standing itself up following passage of CPRA.

We appreciate that certain areas of the rulemaking recognize businesses' need for flexibility, such as the totality of circumstances standard and the concept of the alternative opt-out link. As delineated in these comments, however, the current draft of the rulemaking has many provisions that need further clarifications or revisions to both preserve consumer choice and interests and respect legitimate business operations and functions. Additionally, we are very concerned about provisions of the rulemaking that conflict directly with the plain language of the statute; we respectfully request these be corrected.

1. The enforcement deadline should be extended.

A paramount concern of businesses is the CPPA's enforcement deadline of July 1, 2023. We urge the CPPA to extend the enforcement deadline by 12 to 18 months from the adoption of the final rulemaking.

As noted, even before CPRA's adoption, businesses were struggling with implementation of CCPA. CPRA's added layer has meant even more complexity and questions. Compliance will require businesses to substantially add to resources across – personnel, time and financial. Businesses will need to consult experts, change national and global systems, and adopt technology. These changes require very long runways for businesses.

An extension will also provide time for CPPA and stakeholders to work through questions about this rulemaking and requested revisions to ensure the regulations are workable and businesses fully understand their compliance obligations. This is especially true since the proposed rulemaking contemplates significant new compliance obligations that exceed statutory requirements.

Extending the enforcement deadline is also consistent with the timeframe originally contemplated by the statute under section 1798.185(d) in which the CPRA regulations were to be finalized by July 1, 2022. The delay in the final rulemaking is fully understandable given the Agency needed a reasonable time period to establish. However, the delay has created a great deal of uncertainty for businesses and the compliance landscape has continued to evolve significantly, particularly in light of other jurisdictions adopting privacy laws.

The reasons for extending the enforcement deadline are more than compelling, will facilitate compliance, and will benefit everyone involved.

² CPRA, Cal. Civ. Code. §. 1798.185(a)(19)(C) (emphasis supplied).

2. Opt-Out Preference Signals [Section 7025]

a. Section 7025's mandate of global opt-out signals exceeds statutory authority.

The plain language of CPRA states that honoring global opt-out preference signals is one of two options for businesses, yet proposed section 7025 makes it mandatory. Under CPRA, businesses can either (a) provide clear and conspicuous opt-out links on their website or (b) allow consumers to opt out through a “preference signal sent with the consumer’s consent[.]”³ The CPRA goes out of its way to emphasize the ability of businesses to choose between the two methods, stating:

A business that complies with subdivision (a) is **not required** to comply with subdivision (b). For the purposes of clarity, a business **may elect** whether to comply with subdivision (a) **or** subdivision (b).⁴

Yet, section 7025 at the outset states that businesses “shall” treat any opt-out preference signal as a “valid request” to opt out.⁵ Surprisingly, the rulemaking appears to go out of its way to state that the CPRA is not in fact providing a choice between these two options. Rather, the choice businesses have is whether to process the universal opt-out signal in a “non-frictionless” or “frictionless” manner.⁶ This construct directly contravenes the plain language of the statute and should be eliminated.

We strongly urge the Agency to clarify that honoring opt-out preference signals is optional by, at a minimum, replacing “shall” with “may” at section 7025(b) and (c)(1).

Proposed modifications

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

(c)(1) The business ~~shall~~ may treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device, and, if known, for the consumer.

(e) Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt-out preference signals and providing the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the alternative opt-out link; or (2) processing opt-out preference signals ~~in a frictionless manner~~ in accordance with these regulations and not having to provide the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the alternative opt-out link. ~~It does not give the business the choice between posting the above referenced links or honoring opt-out preference signals. Even if the business posts the above referenced links, the business must still process opt-out preference signals, though it may do so in a non frictionless manner.~~ If a business processes opt-out preference signals ~~in a frictionless manner~~ in accordance with subsections (f) and (g) of this regulation, then it may, but is not required to, provide the above-referenced links.

³ CPRA, Civ. Code § 1798.135(a), (b)(1), (3).

⁴ *Id.* at (b)(3) (emphasis added).

⁵ §. 7025(b), (c).

⁶ § 7025(e).

b. Section 7025 does not follow statutory direction for rulemaking on global opt-out signals.

In addition to wrongly making universal opt-out signals mandatory, section 7025 also appears to ignore several of the six criteria specifically prescribed by CPRA to incorporate into rulemaking for universal opt-out signals.⁷ For example, there does not appear to be any mention in the rulemaking of the requirement that the Agency “ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.”⁸

The rulemaking also has a number of provisions that conflict with the requirement that it “clearly represent a consumer’s intent and [are] free of defaults constraining or presupposing such intent,” and do “not conflict with other commonly used privacy settings or tools that consumers may employ.”⁹

For example, the rulemaking appears to presume that consumers will choose universal opt-out and imposes overly burdensome requirements on businesses to support this presumption. For instance, section 7025(b) does not appear to contemplate giving consumers the ability to turn on or off the global opt-out, which deprives them of full control over their preferences. Similarly, sections 7025(c)(3)-(4) require businesses to accept the universal opt out even if it overrides a prior consumer choice to participate in a financial incentive program and then create new mechanisms to confirm the consumer wishes to remain in the program. The phrase “in a conspicuous manner” in section 7025(c) should also be revised so it conforms to section 7026(f)(4).

Finally, if a business chooses to process universal opt-out signals, the Agency should not require businesses to process preference mechanisms that exceed current available technologies.

The Agency should ensure that all six of the criteria under section 1798.185(a)(19)(A) are addressed by working with stakeholders including the business community and experts versed in preference signal technologies. As businesses have noted repeatedly, universal opt-out signals use technologies that are still developing, and there is yet to be a consensus among experts and stakeholders that these are a reliable, workable, and secure means for conveying consumer choice. The rulemaking process and requirements

⁷ CPRA, Cal. Civ. Code § 1798.185(a)(19)(A):

The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should:

- (i) Ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.
- (ii) Ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer and does not require that the consumer provide additional information beyond what is necessary.
- (iii) Clearly represent a consumer’s intent and be free of defaults constraining or presupposing that intent.
- (iv) Ensure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ.
- (v) Provide a mechanism for the consumer to selectively consent to a business’ sale of the consumer’s personal information, or the use or disclosure of the consumer’s sensitive personal information, without affecting the consumer’s preferences with respect to other businesses or disabling the opt-out preference signal globally.
- (vi) State that in the case of a page or setting view that the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including:
 - (a) Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information.
 - (b) Choice to “Limit the Use of My Sensitive Personal Information.”
 - (c) Choice titled “Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising.”

⁸ CPRA, Cal. Civ. Code § 1798.185(a)(19)(A).

⁹ *Id.*

need to be adjusted to reflect this.

Proposed modifications

§ 7025 (b): A business ~~shall~~ may 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)~~ (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) 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):

(3) 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).

(4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, ~~the business shall notify the consumer that processing the opt-out preference signal would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the consumer does not affirm their intent to withdraw,~~ the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must provide display in a conspicuous manner the status of the consumer's choice in accordance with section 7026, subsection (f)(4).

3. Requests to Opt-Out of Sale/Sharing [Section 7026]

a. The regulation should be prospective only and not apply to downstream parties

The opt-out right should apply prospectively only. It is overly burdensome and impractical to require companies to unravel prior data transactions by requiring that opt-out requests be passed downstream to any other person with whom they previously interacted in connection with the consumer's data. Or alternatively, at most, the requirement should be limited to the third parties with whom the business directly sold or shared the customer's personal data. Also, subdivision (f)(2) is incorporated into (f)(3) and should be eliminated as duplicative.

Proposed modifications

§ 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.

b. The regulation should not require businesses to display customers' opt out choices on their website

Section 7026(f)(4) requires businesses, through a website display, to allow customers to confirm the business has processed their opt-out request. This also appears to exceed statutory requirements and is technologically burdensome. Businesses should have the option to instead provide this information in the consumer's privacy settings with the business.

Proposed modification

§ 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.

4. Restrictions on the Collection and Use of Personal Information [Section 7002]

a. The vague "average person" standard conflicts with statute.

Section 7002(a) ties the standard for what is "reasonably necessary and proportionate" with respect to data collection and use to "what an average consumer would expect when the personal information was collected." This is extremely subjective and impossible to implement, since there are wide variations as to what the average person might expect. It also could allow the Agency to effectively change the consent framework from an opt-out to an opt-in, which contravenes CPRA. The plain language of CPRA ties data collection and use to the *purposes* for collection of the data and includes compatible purposes that are disclosed to the consumer:

(c) A business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the

context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.¹⁰

The foregoing statutory standard also aligns with Virginia, Colorado, and Connecticut which allows interoperability – crucial for sustaining function and operation for multistate businesses. The regulation should be revised to be consistent with the CPRA statute.

Proposed modification:

§ 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~~ notify the consumer in accordance with section 7004 before collecting, using, retaining, and/or sharing the consumer's personal information for any purpose that is ~~unrelated~~ not reasonably necessary and proportionate or incompatible with the purpose(s) for which the personal information collected or processed.

b. The data minimization examples are overly narrow.

The illustrative examples in section 7002(b) are extremely limiting and will threaten innovation. For instance, example (b)(1) disallows data use for any function other than the primary one – even if the other uses are helpful to and desired by the consumer. A mobile flashlight application can only collect or use data to provide lighting and not for other ancillary benefits, such as identifying public areas where street lighting is too dim. The rulemaking should be revised to include an example that illustrates permissible uses of data to improve or expand features that are compatible with or related to the primary purpose.

Proposed modification

§ 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.

5. Contract Requirements for Service Providers and Contractors [Sections 7050-7053]

a. The rulemaking should be consistent with the CPRA liability exemption for third parties.

The current wording of sections 7051(e) and 7053(e) could be construed to create a blanket due diligence and audit requirement for all service providers, contractors, and third parties and indirectly creates liability for businesses in a manner inconsistent with CPRA section 1798.145(i). This section clearly states that businesses are not liable for the violations of their third-party contractors. Due diligence and auditing

¹⁰ CPRA, Cal. Civ. Code §.1798.100(c) (emphasis supplied).

obligations as to third parties should be limited to situations where businesses have reason to know the third party is violating its obligations — rather than an ongoing obligation to confirm the absence of violations.

Proposed modifications

Sections 7051(e) and 7053(e) should be deleted in their entirety or alternatively revised as follows:

§ 7051(e): A business shall take reasonable steps to determine compliance with the terms of the contract with service providers and contractors when the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. ~~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 nor exercises its rights to 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): A business shall take reasonable steps to determine compliance with the terms of the contract with third parties when the business has reason to believe that a third party is using personal information in violation of the CCPA and these regulations. ~~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 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.~~

b. The rulemaking is overly prescriptive with respect to contract provisions.

There are several provisions in this rulemaking that overly prescribe how businesses should draft their contracts and are overly punitive if businesses do not strictly adhere to these detailed requirements. Businesses should be given latitude to reasonably construct their contracts in a manner that requires their service providers to comply with the law. These include:

- While businesses do not object to the requirement to include in contracts the purposes of processing that are authorized and purposes that are prohibited, the rules should not dictate where and how they are placed into a contract. For example, section 7051(a)(3) requires the list of authorized purposes be placed in the same section as prohibited purposes. This will be disruptive and burdensome for many businesses who use standardized or form contracts. The rules should simply state what is required to be included and not dictate in what sections of the contract those obligations appear; the rules should leave contract construction up to businesses.
- Section 7051(a)(10) also adds a new requirement that all service provider contracts include a provision obligating businesses to inform service providers of any consumer request made pursuant to CCPA. This obligation should not be mandated to be included in contracts, as it creates unnecessary additional liability for businesses with the service provider for an obligation where there is already accountability with the Agency.

- Section 7051(c) also proposes to convert all service provider/contractor relationships into third-party relationships if the contract is not fully compliant with the rules. This will trigger a host of additional legal obligations which is punitive and unreasonable. A noncompliant contract should be handled as other violations are handled without unwinding legal relationships between private parties, and there should be a reasonable opportunity for businesses to address contract issues. This rule should be removed.
- Five business days for the service providers/contractors to notify businesses they can no longer meet obligations is too short. Businesses and service providers should be permitted to set a mutually satisfactory notice in a given contract, but if it is going to be prescribed, the rule should provide for at least 10 days.
- The Agency lacks statutory authority to categorically deem all providers of cross-contextual behavioral advertising as third parties under section 7050(c). Whether they are third parties should be defined by the contract terms. Rules that apply to personal information and cross-contextual behavioral advertising provide sufficient protections to consumers.
- Section 7053(a)(1) should be revised to remove the requirement to list specific purposes for which personal information is disclosed in every third-party contract. Businesses may work with numerous vendors

Proposed modifications

Delete § 7050(c) in its entirety.

§ 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(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(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.~~

§ 7053. (a) A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:

(1) Identifies the limited ~~and specified~~ purpose(s) for which the personal information is sold or disclosed. The purpose shall not be described ~~in generic terms, such as~~ **by** referencing the entire contract generally. ~~The description shall be specific.~~

(2) Specifies that the business is disclosing the personal information to the third party only for the limited ~~and specified~~ purposes set forth within the contract and requires the third party to only use it for those limited ~~and specified~~ purposes.

6. Requests to Delete and Correct [Sections 7022-7023]

a. The deletion and correction processing requirements are too burdensome .

We appreciate provisions in the rulemaking that provide businesses with flexibility, such as allowing businesses to “consider the totality of the circumstances,” as it does for reviewing correction requests under section 7023(b). We ask, however, that sections 7022 and 7023 be revised to remove some provisions that will be onerous for businesses.

First, businesses should not be required to provide a consumer with detailed explanations as to why it cannot notify all third parties or is denying a deletion or correction request.¹¹ The rulemaking should also not require businesses to disclose the source of the information the consumer contends is inaccurate, which could expose private contracts.¹²

Additionally, the burden to prove inaccuracy should be on the consumer. It would also be helpful if regulations provided illustrative real-life examples of personal information inaccuracies about which they are most concerned. Finally, businesses should not be required to reprocess repeat access requests.¹³

The rulemaking already gives consumers significant control over their personal information, so it is unnecessary to impose excessively burdensome requirements on businesses.

Proposed modifications

§ 7022(b)(3): Notifying all third parties to whom the business has sold or shared the personal information to delete the consumer’s personal information unless this proves impossible or involves disproportionate effort. ~~If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effort.~~

§ 7022(f): In cases where a business denies a consumer’s request to delete in whole or in part, the business shall do all of the following:

(1) ~~Provide to~~ If applicable, notify the consumer ~~a detailed explanation of the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, or factual basis for contending~~ that compliance would be impossible or involve disproportionate effort, unless prohibited from doing so by law;

§ 7023(b): In determining the accuracy of the personal information that is the subject of a consumer’s request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer’s request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances or if the consumer fails to provide information validating the correct information.

§ 7023(f)(2): If a business claims that complying with the consumer’s request to correct would be impossible or would involve disproportionate effort, the business shall provide notify the consumer ~~a detailed explanation that includes enough facts to give a consumer a meaningful~~

¹¹ § 7022(b), (c), (f)(1), 7023(f).

¹² § 7023(i).

¹³ § 7023(j).

~~understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.~~

~~§ 7023(i): Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business shall provide the consumer with the name of the source from which the business received the alleged inaccurate information.~~

~~§ 7023(j) Upon request, a business shall disclose all the specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b).~~

b. The requirement to send detailed explanations to services providers and contractors is overly burdensome.

The requirement to convey correction and deletion requests to service providers and contractors under the rulemaking forces the business to act as a middleperson between the consumer and any external party that receives the consumer's personal information.¹⁴ While it is reasonable in some situations to require businesses to provide notifications of corrections/deletions, having to relay detailed explanations between service providers/contractors and consumers will be extremely burdensome.¹⁵ The impossible or disproportionate effort standard should preclude this.¹⁶

Proposed modifications

§ 7022(b)(3): Notifying all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. ~~If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effort.~~

§ (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

¹⁴ § 7022(b)(3), 7022(c)(4).

¹⁵ § 7022(c)(4).

¹⁶ § 1798.105(c)(1).

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.

7. Requests to Know [Section 7024]

a. Request to know should be subject to reasonable parameters.

Generally, for requests to know, the consumer should be required to designate the specific period for which information is sought. It is inappropriate for a business to have provide all information sought for unlimited time ranges. Further, businesses should not be required to provide personal information its service providers or contractors have collected unless that information was shared with the business. Businesses should also not be required to provide detailed explanations. This is disproportionate. Finally, the rulemaking should not dictate how businesses work with service providers under section 7024(i).

Proposed modifications

§ 7024(h): In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer on or after January 1, 2022 for a specific time period designated by the consumer, including beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort. That information shall include any personal information that the business's service providers or contractors obtained as a result of providing services to the business and was shared with the business. ~~If a business claims that providing personal information beyond the 12-month period would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort.~~

§ 7024(i): A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to know, ~~including by providing the business the consumer's personal information it has in its possession that it obtained as a result of providing services to the business.~~

8. Dark Patterns [Section 7004]

a. The symmetry choice standard for dark patterns is overly broad and inflexible.

The regulations aimed at preventing dark patterns should focus on practices that constitute consumer fraud, which has been the longstanding and well-developed standard. This approach would target those design practices that deceive consumers into taking a desired action, such as by misleading customers about the consequences of providing or refusing consent.

Additionally, the agency should apply a reasonableness standard and utilize objective criteria. The proposed symmetry choice standard under section 7004 is overly broad, subjective and inflexible. There may be legitimate reasons for imperfect symmetry. The rules should also focus on reducing practices that harm consumers by using objective criteria, rather than subject criteria that can dilute consumer choice or benefit or interfere with function.

Examples of dark patterns regulations that are overly prescriptive or subjective include:

- Under illustrative example (a)(2)(A), rather than requiring the same number of steps to opt out can never exceed those for opt-in, a reasonable basis such as providing information on impacts or ensuring the customer's security should be allowed.
- Example (a)(2)(C) is too rigid. The rulemaking should not mandate that businesses can only provide all-or-nothing choices – “accept all” or “decline all.” Businesses should be able to provide consumers with a choice to choose individualized preferences.
- The examples (a)(3) that yes/no or on/off toggle buttons are confusing seem to discourage utilization of toggle buttons. The rules should simply require businesses to clearly indicate consumer choice in a reasonable manner including when using toggle buttons.
- Example (a)(4)(C) implies that it is incompatible for a business to obtain the consumer's consent to share or sell location data when it is obtaining a consumer's location to provide as service. Inability to bundle these choices would require a business to obtain the consumer's location data multiple times which will degrade user experience and privacy and pose undue operational burdens for businesses.
- Under section 7004(a)(4), architecture requirements should focus on avoidance of deceptive architecture rather than whether it is “manipulative,” “guilting” or “shaming” which are highly subjective terms.
- Section 7004(a)(5) could create liability for businesses for ordinary technical issues or security practices. Again, a reasonableness standard should apply for measuring whether there is improper burden or friction for the consumer.

Proposed modifications include:

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

...

§ 7004(a)(4): Avoid manipulative deceptive language or choice architecture. The methods should not use language or wording that guilts or shames 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 deceptive manipulative and shaming.

(C) It is manipulative misleading 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 not notified of the purposes for 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 notify the consumer to consent to incompatible of other 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.

9. Notice at Collection of Personal Information [Section 7012]

a. Businesses should be permitted to provide personal information and third party information in their privacy policies.

The requirement under section 7012 to provide unique lists of personal information and third parties for each consumer notice will be extremely burdensome and can be addressed more efficiently for businesses and consumers through the businesses' privacy policies.

Businesses can provide details on what type of personal information is collected from consumers in the privacy policy which consumers can navigate by use of clear headings. It will be cumbersome and difficult for businesses to provide a customized link for each consumer for every type of personal information upon collection.¹⁷

With respect to third parties, large companies often use numerous third parties to collect personal information the third parties can be constantly changing. It is too burdensome to track and provide these lists to consumers.¹⁸ Additionally, identifying specific third parties could weaken security and undermine negotiations with service providers. The rules should instead have businesses provide types of third parties utilized in their privacy policies.

For record retention guidelines, businesses do not generally categorize by personal information but instead by record type. The rules could instead have companies identify what personal information is likely to be included in particular record types.

Proposed modifications

§ 7012(e)(5): When a business collects personal information over the telephone or in person, it may provide the notice orally or refer the consumer to the business' website for the notice or offer to email the notice to the consumer.

§ 7012(e)(6): If a business allows third parties to control the collection of personal information, the ~~names of all the~~ link to the privacy policy listing the types of third parties; or in the alternative information about the third parties' business practices.

§ 7012(f): If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link that takes the consumer directly to ~~the specific section of the~~ business's privacy policy that contains the information required in subsection (e)(1) through (6) in a manner that is clearly delineated such as by use of headings. Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.

b. The rules should allow third parties flexibility to align notice with data collection methods.

For third-party businesses that control the collection of data on another business' premises, section 7012(g)(3) should permit third-party businesses to provide notice in a reasonable manner that factors in the method of the 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.

¹⁷ § 7012(c), (f).

¹⁸ § 7012(c)(6).

Proposed modifications

§ 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 at the physical location(s) where it is collecting the personal information in a reasonable format that is consistent with the method of data collection.

10. Notice of Right to Opt-Out of Sale/Sharing of and the “Do Not Sell or Share My Personal Information” Link [Section 7013]

a. The rules should allow notice of opt-out of sale/sharing via business websites.

The regulations require that businesses provide notice to opt-out of sale/sharing in the same way it collects the personal information for that purpose.¹⁹ This will be unduly burdensome for businesses who maintain a website but may collect data by other mean. This exceeds statutory requirements which only require businesses who are online to disclose consumers' rights in their online privacy policy or website.²⁰ The rulemaking should not expand notice obligations beyond the statute.

The rulemaking seems to acknowledge this by allowing a brick and mortar store to provide physical notice in the store, but also with signage that directs them to an online notice.²¹ Similarly, the rules should allow a business collecting personal info over the phone to orally provide notice or direct them to the website, but rules prohibit the latter option.²²

Proposed modifications

§ 7013(e)(3): A business ~~shall~~ may also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow.

(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 or direct the consumer to where the notice can be found online.

(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.

b. Section 7013(h) exceeds statutory authority.

¹⁹ § 7013(e).

²⁰ § 1798.130(a)(5).

²¹ § 7013(e)(3)(A).

²² § 7013(e)(3)(B).

The affirmative consent requirement of section 7013(h) appears nowhere in the statute, conflicts with CPRA's opt-out framework, and should be removed. At a minimum, it should be revised to clarify that it applies to data collected after the effective date of the final rulemaking.

Proposed modification

§ 7013(h): A business shall not sell or share the personal information it collected [after the effective date of this regulation 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.

c. Clarify whether businesses can bifurcate the “Do Not Sell” and “Do Not Share” options.

Section 7013 should be revised to provide businesses more flexibility. Rather than mandating a combined “Do Not Sell or Share My Personal Information Link” as the only option, businesses should be permitted to provide these as two separate links.

11. Limit Sensitive Information and Alternative Opt-Out Links [Sections 7014-7015]

a. Remove the icon requirement from the alternative opt-out link option.

We appreciate the intent described in section 7015(a) which is to give businesses the ability to use a single opt-out link as an alternative to providing the two links for rights to opt-out and limit. However, the requirement that the alternative opt-out link must provide an icon that meets detailed specifications significantly diminishes the ability of businesses to utilize the option due to development challenges.

For example, icon must be the same size as other icons used by the business which might vary from page to page on the website. This means a business may have to create a different icon for each page on a website.

A better approach would be to allow the alternative opt-out link to be in text form without the requirement of an accompanying icon. This format will still provide consumers with a clear link for reviewing and making their privacy choices.

b. Clarify whether to alternative opt-out link is an option if the business does not use any sensitive personal information.

Section 7014 needs to clarify whether a business that does not use sensitive personal information at all can instead use the alternative opt-out links “Your Privacy Choices” or “Your California Privacy Choices.”

c. Consider allowing the alternative opt-out link serve as a single link for all California consumer privacy right choices and rights.

Businesses would like the option to post a single link like “California Privacy Rights” (without the icon requirement) that would take consumers to a portal to learn about and request applicable California privacy rights.

12. Requests to Limit Use and Disclosure of Sensitive Personal Information [Section 7027]

a. The opening paragraph of Section 7027 needs clarifications to avoid conflicts with the statute and rules.

Section 7027(a) needs clarifications to ensure that it does not create confusion or conflict with the statute or other provisions of the section. For example, the reference to “heightened risk of harm” is ambiguous

and could be interpreted to create a new liability standard. This should be deleted or defined, particularly in light of the references to “risk of harm” and “greater risk of harm” in Section 7060(c)(3), which appears to create three distinct categories of consumer harm. The last sentence of this section describing the consumer’s ability to limit also conflicts with exceptions allowing businesses to disclose sensitive personal information without offering the right to limit when for performing services reasonably expected by an average consumer, fraud prevention, and other routine business purposes.

Section 7027(b) conflicts with the statutory exception that treats sensitive personal information that will not be used to infer characteristics about the consumer as personal information.²³ The rulemaking should be revised throughout to incorporate and recognize this exception and provide illustrative examples.

Proposed modification

§ 7027(a): ~~The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer.~~ The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business’s use of sensitive personal information ~~for uses outside of~~ to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, ~~security reasons, fraud prevention, transient use, and other business purposes with some narrowly tailored exceptions, which are~~ set forth in subsection (l). Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section and shall be treated as personal information.

b. Use cases for sensitive personal information should not be preselected for the consumer.

We support the rulemaking’s allowing businesses to present specific use cases for sensitive personal information to consumers, but the Agency should not require that a single option be presented more prominently than the others. This could interfere with customer choice and information. It also conflicts with the Agency’s proposed symmetry standards for consumer choice architecture under section 7004.²⁴

c. Businesses should be able to deny suspicious requests by authorized agents.

Section 7027(i) should be revised to enable businesses to deny requests for sensitive information from authorized agents if there is reasonable suspicion that it is a fraudulent request.

Proposed modification

§ 7027(i): A consumer may use an authorized agent to submit a request to limit on the consumer’s behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer’s signed permission demonstrating that they have been authorized by the consumer to act on the consumer’s behalf ~~or if the business has reasonable suspicion that the request is fraudulent.~~

13. Probable Cause Proceedings [Section 7302]

The draft rules provide for a very broad understanding of probable cause and do not allow businesses the opportunity to cure an alleged violation or to appeal the agency’s probable cause determination. Section

²³ CPRA, Cal. Civ. Code. § 1798.121(d).

²⁴ § 7027(h).

7302 should be revised to provide the alleged violator an opportunity to cure during the 30-day window between receipt of notice of proceeding and the proceeding

14. Agency Investigations and Audits [Section 7304]

a. The audit scope and approach need clearer standards and more flexibility for businesses.

Given that investigations and audits can be time consuming and costly for both the Agency and businesses, we urge the Agency to revise the rulemaking to provide clear and objective bases for any audits and to establish limits. Without these, audits could be unproductive and unnecessarily drain resources, and could also lead to broad fishing expeditions.

The rulemaking should be revised to limit audits to possible violations that are based on reasonable suspicion, and the rules should define “significant risk” under section 7304(b) or provide examples. The proposed regulations should also be confined to audits of businesses, not individuals.

The CPRA provides parameters for audits under section 1798.199.45 that would allow the Agency to incorporate flexibility and a range of enforcement mechanisms into the regulations as other California enforcement bodies have done. For example, the California Public Utilities Commission implements progressive enforcement, beginning with actions such as a notice or warning and only later in the process may impose penalties or file a civil or criminal action.²⁵ This process may not apply if the violation is egregious or widespread.²⁶

The regulations also do not provide for any notice of audits and broadly state they may be announced or unannounced. Paired with this is the draconian consequence that the agency can seek criminal charges against any subject for failure to cooperate during an audit, which is beyond the scope of its authority. As noted above, the rules should provide a more gradual progression of consequences that is commensurate with the issue or violation at hand.

15. Risk assessments need to be addressed in the rulemaking.

The proposed regulations should be revised to provide businesses with more guidance on risk assessments of personal information processing. The CPRA requires businesses to submit these to the Agency on a regular basis under section 1798.185(a)(15)(B) and instructed the Agency to address this obligation in the rulemaking.

16. The rulemaking should provide a grace period for employment records.

With the expiration of the employment records exemption set forth in CPRA section 1798.145(m)(1) set for January 1, 2023, we request that the Agency provide a grace period for enforcement of the rules as applied to employment records. The grace period should match the extension for enforcement of the overall rulemaking requested in section 1 of these comments since the pending rulemaking will impact employment records once the exemption expires. Businesses will need time to apply the rulemaking to employment records and carry out required implementation which will be especially challenging since the opt-out and deletion rights for personal information are incompatible with business functions and other legal obligations.

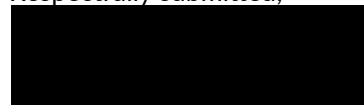
²⁵ CPUC Enforcement Policy, R. M-4846 at 4, November 5, 2020.

²⁶ *Id.*

Conclusion

Regulations that are unclear, burdensome, or exceed statutory authority will give rise to unnecessary and unproductive enforcement actions and litigation, which are costly for everyone including the Agency. The goal of the regulations should be to facilitate implementation of and compliance with CCPA and CPRA with the approach enshrined in CPRA which is to consider the interests and needs of both consumers and businesses.

Respectfully submitted,

A black rectangular redaction box covering the signature of Kyla Christoffersen Powell.

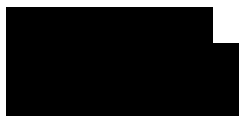
Kyla Christoffersen Powell
President and Chief Executive Officer

From: **Alastair Mactaggart** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CCPA Public Comment [Proposed Rulemaking]
Date: 24.08.2022 01:25:55 (+02:00)
Attachments: CCP comments on Proposed CPRA Regs 8-23-22.docx (4 pages), Draft June 2022
CPRA Regulations -- CCP Comments 8-23-22.pdf (66 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please see two attached documents

Alastair Mactaggart, Chair
Californians for Consumer Privacy



This message may contain information that is privileged or confidential.
If you received this transmission in error, please notify the sender by reply e-mail and delete the message and any attachments. Thank you.



Attn: Ashkan Soltani, Director
 California Privacy Protection Agency
 2101 Arena Blvd
 Sacramento, CA 95834

By Email

August 23, 2022

RE: CCPA Public Comment on Proposed Regulations

Dear Director Soltani:

Attached please find our comments on the July 8, 2022 Proposed Regulations.

We have four overarching “most important” comments, which we explain in more detail below. Additionally, we have provided other input in the form of comments to the attached PDF of the proposed regulations.

The four are:

- 1) **Global Opt-Out, §7025.** We have seen much commentary to the effect that the global opt-out is not mandatory, but is an ‘either/or’ option. Many have suggested, falsely, that CPRA §1798.135 permits businesses to choose *either* to provide the link to opt-out of sale or sharing of personal information, *or* to recognize a universal opt-out signal.

To the contrary, CPRA §1798.135(e) states: *A consumer may authorize another person to opt-out of the sale or sharing of the consumer’s personal information and to limit the use of the consumer’s sensitive personal information on the consumer’s behalf, including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b), indicating the consumer’s intent to opt out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer’s behalf, pursuant to regulations adopted by the Attorney General regardless of whether the business has elected to comply with subdivision (a) or (b).*

§1798.140(u) defines ‘person’ as: *an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.*

Thus a plain English reading of §1798.135(e) is that a consumer *may* authorize (i.e., the consumer is “*allowed to*” authorize—“*may*” gives the consumer *the right* to authorize) another *person* (*person* as in a company, corporation, application, non-profit, etc., including obviously

any application or tool provided by such entity) to opt-out *for* the consumer, i.e. on the consumer's behalf.

And in that case, the business “*shall comply* with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General regardless of whether the business has elected to comply with subdivision (a) or (b)” with the opt-out request.

There is no “choice” here. Regardless of whether the business chooses §1798.135(a) or (b), the business *must* honor the consumer's opt-out request delivered via a global opt-out (presuming that the CPPA has blessed the opt-out protocol); which comes full circle, and means that all businesses *must always comply with* all global opt-out requests.

There is no other reading that makes any sense here, and suggestions to the contrary are simply from Surveillance Economy¹ firms and their defenders, trying to wriggle out of having to comply with consumer choice.

The only choice is whether to post the Do Not Sell/Share link—if a business does, then it can respond as allowed by §1798.121; if it does not, then it cannot respond to the opt-out request, it literally has to treat the consumer as if they showed up without the global opt-out enabled.

CCP recommends that §7025(b) of the proposed regulations **not** be amended.

- 2) **CPRA §1798.100(c), Data Minimization.** §7002 of the Proposed Regulations is excellent, and we support the standard of “what an average consumer would expect.” Rather than enumerate a long list of acceptable uses, we agree with the CPPA that a standard that addresses consumers' reasonable expectations is stronger, since businesses will be forced to spend time thinking through whether a certain type of processing is something their average user would expect. And given the plethora of stories about consumers' health data being shared amongst non-HIPAA-regulated entities, which if it were in the possession of an entity covered by HIPAA would be criminal to disclose, we think this standard is relevant and correct.

We urge the CPPA to interpret the phrase “compatible with the context in which the personal information was collected” as strictly as possible. Businesses litter their privacy policies with blanket statements saying that information they collect from their users can be used any number of ways—a favorite is along the lines of allowing sharing with partners to “improve our service;” taken literally, these often allow a business to sell personal information and argue that making more money helps them improve the service they offer consumers.

- 3) **CPRA §1798.185(d), Timing.** We urge the CPPA not to delay implementation or enforcement of CPRA. The statute is clear, there is no exception for enforcement, draft regulations are promulgated and can be finalized before Jan 1, 2023. Businesses have had since November

¹ Professor Shoshana Zuboff's term

2020 to realize that the landscape has changed permanently around the personal information economy in California, and regardless of the exact final form of the regulations, have known that the untrammelled trafficking of their users' most intimate information, was coming to an end in California in 2023. So it is highly disingenuous for them to argue now that because they don't know the exact language the regulations will take, they cannot comply with CPRA next year.

The architecture is not complicated: CPRA, in most cases just like CCPA, gives consumers the right to stop the sale or sharing of their information; the right to delete it, the right to correct it, the right to access it.

Businesses can and must comply with the CPRA regs—in most cases, CPRA simply clarifies or underlines what businesses should already be doing as a result of CCPA.

- 4) **Opt-Out Preference Signals, proposed §7025(c)(2):** We feel strongly that the CPPA should not allow businesses to request additional information, when a consumer opts-out of the sale of their Personal Information, or the use of the Sensitive Personal Information.

We feel that the opt-out preference signal should be designed with zero friction. A pop-up asking consumers to provide additional info will annoy consumers and impair user experience, especially compared to a user who does not employ the opt-out.

CCP suggests the regs require the two user experiences be identical, whether a consumer is opted-out or not.

We think the 'online' opt-out should be designed such that (a) it tells the business, don't sell any information from *this* session, *plus* (b) don't sell any information you can *reasonably link to this consumer* from this visit, ie that the business *already* holds with respect to the consumer.

We suggest including language from 1798.130 (a)(3)(B)(i), in which case this regulation would read: "The business shall not require a consumer to provide additional information beyond what is necessary to send the signal, *and shall associate the information provided by the consumer in the opt-out request, to any personal information previously collected by the business about the consumer*, and shall thereafter refrain from selling or sharing such information."

This would put the onus on the business to stop the sale of the consumer's PI if they can (or normally would) link the device/browser ID to *any other* info the business possesses about the consumer (for example, if they routinely, probabilistically choose to associate consumer info with info they are 99% sure, but not 100% sure, is that same consumer's, this insert would cover that method of evasion).

This language would eliminate sale from the *current* session, plus any *other* info held by the business about the consumer--which CCP sees as the vast majority of the problem.

If this regulation is put in place, CCP is concerned that businesses will impose a popup asking for name, email etc. every time a consumer opts out of the sale/sharing of their information, which may make consumers less willing to enable DNS/S, since all they want is their information not sold--not to have to provide *additional* information.

To address the concern that businesses sell information offline, i.e. not just the information obtained from an internet visit, we suggest requiring a link in the business' privacy policy that allows consumers to provide additional data beyond what a browsing visit would supply, including name, address, etc., which would prevent the business from selling that information. This would also allow a place/mechanism for third party apps used by the consumer, to go and opt-out on the consumer's behalf.

Please see, additionally, our comments in the form of comments to the PDF of the proposed regulations.

Yours sincerely

Alastair Mactaggart, Chair

CALIFORNIA PRIVACY PROTECTION AGENCY

TITLE 11. LAW

DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY

CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

TEXT OF PROPOSED REGULATIONS

The original text published in the California Code of Regulations has no underline. Changes are illustrated by single blue underline for proposed additions and ~~single red strikethrough~~ for proposed deletions.

Article 1. GENERAL PROVISIONS

§ 7000. Title and Scope.

- (a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.
- (b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.

Note: Authority cited: Sections 1798.175 and 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, ~~and 1798.185~~, 1798.199.40, 1798.199.45, 1798.199.50, 1798.199.55, and 1798.199.65, Civil Code.

§ 7001. Definitions.

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

- ~~(a) “Affirmative authorization” means an action that demonstrates the intentional decision by the consumer to opt in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer’s personal information in accordance with the methods set forth in section 7070. For consumers 13 years of age and older, it is demonstrated through a two step process whereby the consumer shall first, clearly request to opt in and then second, separately confirm their choice to opt in.~~
- (a) “Agency” means the California Privacy Protection Agency established by Civil Code section 1798.199.10 et seq.

- (b) “Attorney General” means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.
- (c) “Authorized agent” means a natural person or a business entity ~~registered with the Secretary of State to conduct business in California~~ that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.
- (d) “Categories of sources” means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.
- (e) “Categories of third parties” means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.
- (f) “CCPA” means the California Consumer Privacy Act of 2018, Civil Code section 1798.100 *et seq.*
- (g) “COPPA” means the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6508 and 16 Code of Federal Regulations part 312.5.
- (h) “Disproportionate effort” within the context of a business responding to a consumer request means the time and/or resources expended by the business to respond to the individualized request significantly outweighs the benefit provided to the consumer by responding to the request. For example, responding to a consumer request to know may require disproportionate effort when the personal information which is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and would not impact the consumer in any material manner. In contrast, the benefit to the consumer of responding to a request to correct inaccurate information that the business uses and/or sells may be high because it could have a material impact on the consumer, such as the denial of services or opportunities. Accordingly, in order for the business to claim “disproportionate effort,” the business would have to demonstrate that the time and/or resources needed to correct the information would be significantly higher than that material impact on the consumer. A business that has failed to put in place adequate processes and procedures to comply with consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer’s request requires disproportionate effort.
- (i) ~~(h)~~ “Employment benefits” means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer’s employer.
- (j) ~~(i)~~ “Employment-related information” means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145,

subdivision ~~(h)~~(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.

~~(k) “Household” means a person or group of people who: (1) reside at the same address; (2) share a common device or the same service provided by a business; and (3) are identified by the business as sharing the same group account or unique identifier.~~

~~(k)~~ ~~(j)~~ “Financial incentive” means a program, benefit, or other offering, including payments to consumers, ~~related to~~ for the collection, ~~deletion, retention, or sale, or sharing~~ of personal information. Price or service differences are types of financial incentives.

(l) “First party” means the consumer-facing business with which the consumer intends and expects to interact.

(m) “Frictionless manner” means a business’s processing of an opt-out preference signal that complies with the requirements set forth in section 7025, subsection (f).

~~(n)~~ ~~(f)~~ “Notice at collection” means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in these regulations.

(o) “Notice of right to limit” means the notice given by a business informing consumers of their right to limit the use of the consumer’s sensitive personal information as required by Civil Code sections 1798.121 and 1798.135 and specified in these regulations.

~~(p)~~ ~~(m)~~ “Notice of right to opt-out of sale/sharing” means the notice given by a business informing consumers of their right to opt-out of the sale or sharing of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.

~~(q)~~ ~~(n)~~ “Notice of financial incentive” means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.

(r) “Opt-out preference signal” means a signal that is sent by a platform, technology, or mechanism, on behalf of the consumer, that communicates the consumer choice to opt-out of the sale and sharing of personal information and that complies with the requirements set forth in section 7025, subsection (b).

~~(s)~~ ~~(e)~~ “Price or service difference” means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, ~~or sale~~ or sharing of personal information, ~~including through the use of discounts, financial payments, or other benefits or penalties;~~ or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, ~~or sale~~ or sharing of personal information, including the denial of goods or services to the consumer.

~~(t)~~ ~~(p)~~ “Privacy policy,” as referred to in Civil Code section 1798.130, subdivision (a)(5), means the statement that a business shall make available to consumers describing the business’s practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information.

- (u) “Request to correct” means a consumer request that a business correct inaccurate personal information that it maintains about the consumer, pursuant to Civil Code section 1798.106.
- (v) ~~(+)~~ “Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.
- (w) ~~(+)~~ “Request to know” means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections ~~1798.100~~, 1798.110, or 1798.115. It includes a request for any or all of the following:
- (1) Specific pieces of personal information that a business has collected about the consumer;
 - (2) Categories of personal information it has collected about the consumer;
 - (3) Categories of sources from which the personal information is collected;
 - (4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;
 - (5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
 - (6) The business or commercial purpose for collecting or selling personal information.
- (x) “Request to limit” means a consumer request that a business limit the use and disclosure of the consumer’s sensitive personal information, pursuant to Civil Code section 1798.121, subdivision (a).
- (y) ~~(+)~~ “Request to opt-in to sale/sharing” means ~~the affirmative authorization an action demonstrating that the consumer has consented to the business’s sale or sharing of that the business may sell~~ personal information about the consumer by a parent or guardian of a consumer less than 13 years of age, ~~or~~ by a consumer at least 13 ~~and less than 16~~ years of age, ~~or by a consumer who had previously opted out of the sale of their personal information.~~
- (z) ~~(+)~~ “Request to opt-out of sale/sharing” means a consumer request that a business ~~not~~ neither sell ~~nor share~~ the consumer’s personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).
- (aa) “Right to correct” means the consumer’s right to request a business to correct inaccurate personal information that it maintains about the consumer as set forth in Civil Code section 1798.106.
- (bb) “Right to delete” means the consumer’s right to request that a business delete personal information about the consumer that the business has collected from the consumer as set forth in Civil Code section 1798.105.

- (cc) “Right to know” means the consumer’s right to request that a business disclose personal information that it has collected, sold, or shared about the consumer as set forth in Civil Code sections 1798.110 and 1798.115.
- (dd) “Right to limit” means the consumer’s right to request that the business limit the use and disclosure of a consumer’s sensitive personal information as set forth in Civil Code section 1798.121.
- (ee) “Right to opt-out of sale/sharing” means the consumer’s right to direct a business that sells or shares personal information about the consumer to third parties to stop doing so as set forth in Civil Code section 1798.120.
- (ff) ~~(+)~~ “Signed” means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 *et seq.*
- (gg) ~~(+)~~ “Third-party identity verification service” means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 5 regarding ~~requests to know and~~ requests to delete, requests to correct, or requests to know.
- (hh) “Unstructured” as it relates to personal information means personal information that is not organized in a pre-defined manner, such as text, video files, and audio files.
- (ii) ~~(w)~~ “Value of the consumer’s data” means the value provided to the business by the consumer’s data as calculated under section 7081.
- (jj) ~~(*)~~ “Verify” means to determine that the consumer making a ~~request to know or~~ request to delete, ~~request to correct, or request to know~~ is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer’s parent or legal guardian.

Note: Authority cited: Sections 1798.175 and 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, ~~and~~ 1798.185, 1798.199.40, 1798.199.45, 1798.199.50, 1798.199.55, and 1798.199.65, Civil Code.

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

- (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. 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.

(b) Illustrative examples follow.

- (1) Business A provides a mobile flashlight application. 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 is not within the reasonable expectations of an average consumer, nor is it reasonably necessary and proportionate to achieve the purpose of providing a flashlight function.
- (2) Business B provides cloud storage services for consumers. An average consumer expects that the purpose for which the personal information is collected is to provide those cloud storage services. Business B may use the personal information uploaded by the consumer to improve the cloud storage services provided to and used by the consumer because it is reasonably necessary and proportionate to achieve the purpose for which the personal information was collected. However, Business B should not use the personal information to research and develop unrelated or unexpected new products or services, such as a facial recognition service, without the consumer's explicit consent because such a use is not reasonably necessary, proportionate, or compatible with the purpose of providing cloud storage services. In addition, if a consumer deletes their account with Business B, Business B should not retain files the consumer stored in Business B's cloud storage service because such retention is not reasonably necessary and proportionate to achieve the purpose of providing cloud storage services.
- (3) Business C is an internet service provider that collects consumer personal information, including geolocation information, in order to provide its services. Business C may use the geolocation information for compatible uses, such as tracking service outages, determining aggregate bandwidth use by location, and related uses that are reasonably necessary to maintain the health of the network. However, Business C should not sell to or share consumer geolocation information with data brokers without the consumer's explicit consent because such selling or sharing is not reasonably necessary and proportionate to provide internet services, nor is it compatible or related to the provision of internet services.
- (4) Business D is an online retailer that collects personal information from consumers who buy its products in order to process and fulfill their orders. Business D's provision of the consumer's name, address, and phone number to Business E, a delivery company, is compatible and related to the reasonable expectations of the consumer when this personal information is used for the purpose of shipping the product to the consumer. However, Business E's use of the consumer's personal information for the marketing of other businesses' products would not be necessary and proportionate, nor compatible with the consumer's expectations. Business E would have to obtain the consumer's explicit consent to do so.

- (c) A business shall not collect categories of personal information other than those disclosed in its notice at collection in accordance with the CCPA and section 7012. If the business intends to collect additional categories of personal information or intends to use the personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, the business shall provide a new notice at collection. However, any additional collection or use of personal information shall comply with subsection (a).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.106, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

§ 7003. Requirements for Disclosures and Communications to Consumers.

- (a) Disclosures and communications to consumers shall be easy to read and understandable to consumers. For example, they shall use plain, straightforward language and avoid technical or legal jargon.
- (b) Disclosures required under Article 2 shall also:
- (1) Use a format that makes the disclosure readable, including on smaller screens, if applicable.
 - (2) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
 - (3) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.
- (c) For websites, a conspicuous link required under the CCPA or these regulations shall appear in a similar manner as other links used by the business on its homepage. For example, the business shall use a font size and color that is at least the approximate size or color as other links used by the business on its homepage.
- (d) For mobile applications, a conspicuous link shall be accessible within the application, such as through the application's settings menu. It shall also be included in the business's privacy policy, which must be accessible through the mobile application's platform page or download page.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130 and 1798.135, Civil Code.

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

- (a) Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles.
- (1) Easy to understand. The methods shall use language that is easy for consumers to read and understand. When applicable, they shall comply with the requirements for disclosures to consumers set forth in section 7003.
 - (2) Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be longer than the path to exercise a less privacy-protective option. Illustrative examples follow.
 - (A) A business's process for submitting a request to opt-out of sale/sharing shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out of sale/sharing is measured from when the consumer clicks on the "Do Not Sell or Share My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.
 - (B) A choice to opt-in to the sale of personal information that only provides the two choices, "Yes" and "Ask me later," is not equal or symmetrical because there is no option to decline the opt-in. "Ask me later" implies that the consumer has not declined but delayed the decision and that the business will continue to ask the consumer to opt-in. An equal or symmetrical choice would be "Yes" and "No."
 - (C) A website banner that serves as a method for opting out of the sale of personal information that only provides the two choices, "Accept All" and "More Information," or "Accept All" and "Preferences," is not equal or symmetrical because the method allows the consumer to "Accept All" in one step, but requires the consumer to take additional steps to exercise their right to opt-out of the sale or sharing of their personal information. An equal or symmetrical choice would be "Accept All" and "Decline All."
 - (D) A choice where the "yes" button is more prominent (*i.e.*, larger in size or in a more eye-catching color) than the "no" button is not symmetrical.
 - (E) A choice where the option to participate in a financial incentive program is selected by default or featured more prominently (*i.e.*, larger in size or in a more eye-catching color) than the choice not to participate in the program is neither equal nor symmetrical.

- (3) Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer's choice. Illustrative examples follow.
- (A) Giving the choice of "Yes" or "No" next to the statement "Do Not Sell or Share My Personal Information" is a double negative and a confusing choice for a consumer.
 - (B) Toggles or buttons that state "on" or "off" may be confusing to a consumer and may require further clarifying language.
 - (C) Unintuitive placement of buttons to confirm a consumer's choice may be confusing to the consumer. For example, it is confusing to the consumer when a business at first consistently offers choices in the order of Yes, then No, but then offers choices in the opposite order—No, then Yes—when asking the consumer something that would benefit the business and/or contravene the consumer's expectation.
- (4) Avoid manipulative language or choice architecture. The methods should not use language or wording that guilts or shames the consumer into making a particular choice or bundles consent so as to subvert the consumer's choice. Illustrative examples follow.
- (A) When offering a financial incentive, pairing choices such as, "Yes" (to accept the financial incentive) with "No, I like paying full price" or "No, I don't want to save money," is manipulative and shaming.
 - (B) Requiring the consumer to click through 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.
- (5) Easy to execute. The business shall not add unnecessary burden or friction to the process by which the consumer submits a CCPA request. Methods should be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request. Illustrative examples follow.

- (A) Upon clicking the “Do Not Sell or Share My Personal Information” link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.
- (B) Circular or broken links, and nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this regulation.
- (C) Businesses that require the consumer to unnecessarily wait on a webpage as the business processes the request may be in violation of this regulation.
- (b) A method that does not comply with subsection (a) may be considered a dark pattern. Any agreement obtained through the use of dark patterns shall not constitute consumer consent. For example, a business that uses dark patterns to obtain consent from a consumer to sell their personal information shall be in the position of never having obtained the consumer’s consent to do so.
- (c) A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business’s intent.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

ARTICLE 2. NOTICES REQUIRED DISCLOSURES TO CONSUMERS

§ 7010. Overview of Required Notices-Disclosures.

- (a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 7011.
- (b) A business that controls the collection of a consumer’s ~~collects~~ personal information ~~from a consumer~~ shall provide a notice at collection in accordance with the CCPA and section 7012.
- (c) Except as set forth in section 7025, subsection (g), a ~~A~~ business that sells or shares personal information shall provide a notice of right to opt-out of sale/sharing or the alternative opt-out link in accordance with the CCPA and sections 7013 and 7015.
- (d) A business that uses or discloses a consumer’s sensitive personal information for purposes other than those specified in section 7027, subsection (l), shall provide a notice of right to limit or the alternative opt-out link in accordance with the CCPA and sections 7014 and 7015.
- (e) A business that offers a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and section 7016.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130 and 1798.135, Civil Code.

§ 7011. Privacy Policy.

- (a) ~~Purpose and General Principles (1)~~ The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, ~~disclosure, and sale,~~ sharing, and retention of personal information. It shall also inform consumers about and of the rights of consumers they have regarding their personal information and provide any information necessary for them to exercise those rights.
- (b) The privacy policy shall comply with section 7003, subsections (a) and (b).
- (c) ~~(2)~~ The privacy policy shall ~~be designed and presented in a way that is easy to read and understandable to consumers. The policy shall:~~
- ~~(A) Use plain, straightforward language and avoid technical or legal jargon.~~
 - ~~(B) Use a format that makes the policy readable, including on smaller screens, if applicable.~~
 - ~~(C) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.~~
 - ~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format. (E) Be available in a format that allows a consumer to print it out as a document.~~
- (d) ~~(b)~~ The privacy policy shall be posted online through a conspicuous link that complies with section 7003, subsections (c) and (d), using the word "privacy" on the business's website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application shall ~~may~~ include a link to the privacy policy in the application's settings menu.
- (e) ~~(e)~~ The privacy policy shall include the following information:
- (1) A comprehensive description of the business's online and offline practices regarding the collection, use, sale, sharing, and retention of personal information, which includes the following:

- (A) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described using the specific terms set forth in Civil Code section 1798.140, subdivisions (v)(1)(A) to (K) and (ae)(1) to (9). To the extent that the business has discretion in its description, the business shall describe the category in a manner that provides consumers a meaningful understanding of the information being collected.
 - (B) Identification of the categories of sources from which the personal information is collected.
 - (C) Identification of the specific business or commercial purpose for collecting personal information from consumers. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected.
 - (D) Identification of the categories of personal information, if any, that the business has sold or shared to third parties in the preceding 12 months. If the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall disclose that fact.
 - (E) For each category of personal information identified in subsection (e)(1)(D), the categories of third parties to whom the information was sold or shared.
 - (F) Identification of the specific business or commercial purpose for selling or sharing consumers' personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is sold or shared.
 - (G) A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.
 - (H) Identification of the categories of personal information, if any, that the business has disclosed for a business purpose to third parties in the preceding 12 months. If the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.
 - (I) For each category of personal information identified in subsection (e)(1)(H), the categories of third parties to whom the information was disclosed.
 - (J) Identification of the specific business or commercial purpose for disclosing the consumer's personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is disclosed.
 - (K) A statement regarding whether or not the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (I).
- (2) An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes the following:

- (A) The right to know what personal information the business has collected about the consumer, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses personal information, and the specific pieces of personal information the business has collected about the consumer;
 - (B) The right to delete personal information that the business has collected from the consumer, subject to certain exceptions;
 - (C) The right to correct inaccurate personal information that a business maintains about a consumer;
 - (D) If the business sells or shares personal information, the right to opt-out of the sale or sharing of their personal information by the business;
 - (E) If the business uses or discloses sensitive personal information for reasons other than those set forth in section 7027, subsection (l), the right to limit the use or disclosure of sensitive personal information by the business; and
 - (F) The right not to receive discriminatory treatment by the business for the exercise of privacy rights conferred by the CCPA, including an employee's, applicant's, or independent contractor's right not to be retaliated against for the exercise of their CCPA rights.
- (3) An explanation of how consumers can exercise their CCPA rights and consumers can expect from that process, which includes the following:
- (A) An explanation of the methods by which the consumer can exercise their CCPA rights;
 - (B) Instructions for submitting a request under the CCPA, including any links to an online request form or portal for making such a request, if offered by the business;
 - (C) If the business sells or shares personal information, and is required to provide a notice of right to opt-out of sale/sharing, the contents of the notice of right to opt-out of sale/sharing or a link to that notice in accordance with section 7013, subsection (f);
 - (D) If the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (l), and is required to provide a notice of right to limit, the contents of the notice of right to limit or a link to that notice in accordance with section 7014, subsection (f);
 - (E) A general description of the process the business uses to verify a consumer request to know, request to delete, and request to correct, when applicable, including any information the consumer must provide;
 - (F) Explanation of how an opt-out preference signal will be processed for the consumer (i.e., whether the signal applies to the device, browser, consumer

account, and/or offline sales, and in what circumstances) and how the consumer can use an opt-out preference signal;

- (G) If the business processes opt-out preference signals in a frictionless manner, information on how consumers can implement opt-out preference signals for the business to process in a frictionless manner;
 - (H) Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf;
 - (I) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 7070 and 7071; and
 - (J) A contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.
- (4) Date the privacy policy was last updated.
- (5) If subject to the data reporting requirements set forth in section 7102, the information required under section 7102, or a link to such information.
- ~~(1) Right to Know About Personal Information Collected, Disclosed, or Sold:~~
- ~~a. Explanation that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.~~
 - ~~b. Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the business.~~
 - ~~c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.~~
 - ~~d. Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.~~
 - ~~e. Identification of the categories of sources from which the personal information is collected.~~
 - ~~f. Identification of the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.~~
 - ~~g. Disclosure or Sale of Personal Information:~~
 - ~~1. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months.~~

~~2. For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.~~

~~3. Statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16 years of age.~~

~~(2) Right to Request Deletion of Personal Information.~~

~~a. Explanation that the consumer has a right to request the deletion of their personal information collected by the business.~~

~~b. Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the business.~~

~~c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.~~

~~(3) Right to Opt Out of the Sale of Personal Information.~~

~~a. Explanation that the consumer has a right to opt out of the sale of their personal information by a business.~~

~~b. Statement regarding whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt out or a link to it in accordance with section 7013.~~

~~(4) Right to Non Discrimination for the Exercise of a Consumer's Privacy Rights.~~

~~a. Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.~~

~~(5) Authorized Agent.~~

~~a. Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.~~

~~(6) Contact for More Information.~~

~~a. A contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.~~

~~(7) Date the privacy policy was last updated.~~

~~(8) If subject to the requirements set forth in section 7102, subsection (a), the information compiled in section 7102, subsection (a)(1), or a link to it.~~

~~(9) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 7070 and 7071.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections [1798.100](#), [1798.105](#), [1798.106](#), [1798.110](#), [1798.115](#), [1798.120](#), [1798.121](#), [1798.125](#), ~~and~~ [1798.130](#) [and 1798.135](#), Civil Code.

§ 7012. Notice at Collection of Personal Information.

- (a) ~~Purpose and General Principles (1)~~ The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, ~~and the purposes for which the personal information will be used.~~ is collected or used, and whether that information is sold or shared, so that consumers can exercise meaningful control over the business's use of their personal information. Meaningful control in this context means to provide consumers with the opportunity to choose how to engage with the business in light of its information practices. For example, upon receiving the notice at collection, the consumer should have all the information necessary to choose whether or not to engage with the business, or to direct the business not to selling or sharing their personal information and to limit the use and disclosure of their sensitive personal information.
- ~~(2) The notice at collection shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:~~
- ~~(A) Use plain, straightforward language and avoid technical or legal jargon.~~
 - ~~(B) Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.~~
 - ~~(C) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.~~
 - ~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.~~
- (b) The notice at collection shall comply with section 7003, subsections (a) and (b).
- (c) (3) The notice at collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow.÷
- (1) (A) When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.
 - (2) When a business collects consumers' personal information through a webform, it may post a conspicuous link to the notice in close proximity to the fields in which the consumer inputs their personal information, or in close proximity to the button by which the consumer submits their personal information to the business.
 - (3) (B) When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.

(4) ~~(C)~~ When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.

(5) ~~(D)~~ When a business collects personal information over the telephone or in person, it may provide the notice orally.

~~(4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just in time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just in time notice, such as through a pop up window when the consumer opens the application, that contains the information required by this subsection.~~

~~(5) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.~~

(d) ~~(6)~~ If a business does not give the notice at collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

(e) ~~(b)~~ A business shall include the following in its notice at collection:

(1) A list of the categories of personal information about consumers, including categories of sensitive personal information, to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

(2) The ~~business or commercial~~ purpose(s) for which the categories of personal information, including categories of sensitive personal information, are collected ~~will be and~~ used.

(3) Whether the category of personal information identified in subsection (e)(1) is sold or shared.

(4) The length of time the business intends to retain each category of personal information identified in subsection (e)(1), or if that is not possible, the criteria used to determine the period of time it will be retained.

(5) ~~(3)~~ If the business sells or shares personal information, the link to the notice of right to opt-out of sale/sharing ~~titled "Do Not Sell or Share My Personal Information" required by section 7026, subsection (a)~~, or in the case of offline notices, where the webpage can be found online.

(6) If a business allows third parties to control the collection of personal information, the names of all the third parties; or, in the alternative, information about the third parties' business practices.

- (7) ~~(4)~~ A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online.
- (f) ~~(e)~~ If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection ~~(b)~~(e)(1) through (6). Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.
- (g) Third Parties that Control the Collection of Personal Information.
- (1) For purposes of giving notice at collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a notice at collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a notice at collection.
- (A) This section shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing. If a consumer makes a request to opt-out of sale/sharing with the first party, both the first party and third parties controlling the collection of personal information shall comply with sections 7026, subsection (f), and 7052, subsection (a).
- (2) A first party that allows another business, acting as a third party, to control the collection of personal information from a consumer shall include in its notice at collection the names of all the third parties that the first party allows to collect personal information from the consumer. In the alternative, a business, acting as a third party and controlling the collection of personal information, may provide the first party information about its business practices for the first party to include in the first party's notice at collection.
- (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 at the physical location(s) where it is collecting the personal information.
- (4) Illustrative examples follow.
- (A) Business F allows Business G, an analytics business, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its notice at collection, which shall identify Business G as a third party authorized to collect personal information from the consumer or information about Business G's information practices, on the introductory page

of its website and on all webpages where personal information is collected. Business G shall provide a notice at collection on its homepage.

- (B) Business H, a coffee shop, allows Business I, a business providing wi-fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the notice at collection for Business H can be found online. Business H's notice at collection shall identify Business I as a third party authorized to collect personal information from the consumer or include information about Business I's practices in its notice. In addition, Business I shall post its own notice at collection on the first webpage or other interface consumers see before connecting to the wi-fi services offered.
- (C) Business J, a car rental business, allows Business M to collect personal information from consumers within the vehicles Business K rents to consumers. Business J may give its notice at collection, which shall identify Business K as a third party authorized to collect personal information from the consumer or include information about Business K's practices, to the consumer at the point of sale, i.e., at the rental counter, either in writing or orally. Business K may provide its own notice at collection within the vehicle, such as through signage on the vehicle's computer dashboard directing consumers to where the notice can be found online. Business K shall also provide a notice at collection on its homepage.
- (h) ~~(d)~~ A business that ~~does not~~ neither collects nor controls the collection of personal information directly from the consumer does not need to provide a notice at collection to the consumer if it ~~does not~~ neither sells nor shares the consumer's personal information.
- (i) ~~(e)~~ A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 *et seq.* that does not collect personal information directly from the consumer does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out of sale/sharing.
- (j) ~~(f)~~ A business collecting employment-related information shall comply with the provisions of section 7012, except ~~with regard to the following: (1) The notice at collection of employment-related information does not need to include the link or web address to the link titled "Do Not Sell My Personal Information". (2) The~~ that the notice at collection of employment-related information is not required to provide a link to the business's privacy policy.
- (k) ~~(g)~~ Subsection ~~(f)~~ (j) shall become inoperative on January 1, ~~2021~~ 2023, unless the CCPA is amended otherwise.

Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.99.82, 1798.100, 1798.115, 1798.120, 1798.121, 1798.145 and 1798.185, Civil Code.

§ 7013. Notice of Right to Opt-Out of Sale/~~Sharing~~ ~~of~~ and the “Do Not Sell or Share My Personal Information” Link.

- (a) ~~Purpose and General Principles (1)~~ The purpose of the notice of right to opt-out of sale/sharing is to inform consumers of their right to direct a business that sells or shares their personal information to stop selling or sharing their personal information and to provide them with the opportunity to exercise that right. The purpose of the “Do Not Sell or Share My Personal Information” link is to immediately effectuate the consumer’s right to opt-out of sale/sharing, or in the alternative, direct the consumer to the notice of right to opt-out of sale/sharing. Accordingly, clicking the business’s “Do Not Sell or Share My Personal Information” link will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.
- ~~(2) The notice of right to opt out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:~~
- ~~(A) Use plain, straightforward language and avoid technical or legal jargon.~~
 - ~~(B) Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.~~
 - ~~(C) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.~~
 - ~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.~~
- (b) The notice of right to opt-out of sale/sharing shall comply with section 7003, subsections (a) and (b).
- (c) The “Do Not Sell or Share My Personal Information” 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 homepages.
- (d) In lieu of posting the “Do Not Sell or Share My Personal Information” link, a business may provide an alternative opt-out link in accordance with section 7015 or process opt-out preference signals in a frictionless manner in accordance with section 7025, subsections (f) and (g). The business must still post a notice of right to opt-out of sale/sharing in accordance with these regulations.
- (e) ~~(b)~~ A business that sells or shares the personal information of consumers shall provide the notice of right to opt-out of sale/sharing to consumers as follows:
- (1) A business shall post the notice of right to opt-out of sale/sharing on the ~~i~~internet webpage to which the consumer is directed after clicking on the “Do Not Sell or Share

My Personal Information” link ~~on the website homepage or the download or landing page of a mobile application. In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application’s settings menu.~~ The notice shall include the information specified in subsection (e) or be a link that takes the consumer directly to the specific section of the business’s privacy policy that contains the same information. If clicking on the “Do Not Sell or Share My Personal Information” link immediately effectuates the consumer’s right to opt-out of sale/sharing or if the business processes opt-out preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.

- (2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out of sale/sharing. That method shall comply with the requirements set forth in section 7004-subsection (a)(2).

- (3) A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow.

(A) A business that sells or shares personal information that it collects in the course of interacting with consumers offline, such as in a brick-and-mortar store, shall also inform consumers by an offline method of their right to opt out and provide instructions on how to submit a request to opt out provide notice through an offline method, e.g., —~~Illustrative examples follow: (A) A business that sells or shares personal information that it collects from consumers in a brick and mortar store may inform consumers of their right to opt out~~ on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice opt-out information can be found online.

(B) A business that sells or shares personal information that it collects over the phone ~~may~~ shall provide notice ~~inform consumers of their right to opt out~~ orally during the call when the information is collected.

(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 while using the device.

(D) A business that sells or shares personal information that it collects in augmented or virtual reality, such as through gaming devices or mobile applications, shall provide notice in a manner that ensures that the consumer will encounter the notice while in the augmented or virtual reality environment.

(f) (e) — A business shall include the following in its notice of right to opt-out of sale/sharing:

- (1) A description of the consumer’s right to opt-out of the sale or sharing of their personal information by the business; and

- (2) Instructions on how the consumer can submit a request to opt-out of sale/sharing. If notice is provided online, the notice shall include t~~The interactive form by which the consumer can submit their request to opt-out of sale/sharing online, as required by section 7026, subsection (a)(1). -or-~~If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to opt-out of sale/sharing.~~and~~
- ~~(3) Instructions for any other method by which the consumer may submit their request to opt out.~~
- ~~(g) (4)~~ A business does not need to provide a notice of right to opt-out of sale/sharing or the “Do Not Sell or Share My Personal Information” link if:
- (1) It does not sell or share personal information; and
 - (2) It states in its privacy policy that it does not sell or share personal information.
- ~~(h) (e)~~ A business shall not sell or share the personal information it collected during the time the business did not have a notice of right to opt-out of sale/sharing posted unless it obtains the affirmative authorization consent of the consumer.
- ~~(f) Opt Out Icon.~~
- ~~(1) The following opt out icon may be used in addition to posting the notice of right to opt out, but not in lieu of any requirement to post the notice of right to opt out or a “Do Not Sell or Share My Personal Information” link as required by Civil Code section 1798.135 and these regulations.~~



- ~~(2) The icon shall be approximately the same size as any other icons used by the business on its webpage.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 7014. Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link.

- (a) The purpose of the notice of right to limit is to inform consumers of their right to limit a business’s use and disclosure of their sensitive personal information and to provide them with the opportunity to exercise that right. The purpose of the “Limit the Use of My Sensitive Personal Information” link is to immediately effectuate the consumer’s right to limit, or in the alternative, direct the consumer to the notice of right to limit. Accordingly, clicking the business’s “Limit the Use of My Sensitive Personal Information” link will either have the immediate effect of limiting the use and disclosure of the consumer’s sensitive personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.
- (b) The notice of right to limit shall comply with section 7003, subsections (a) and (b).

- (c) The “Limit the Use of My Sensitive Personal Information” 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 homepages.
- (d) In lieu of posting the “Limit the Use of My Sensitive Personal Information” link, a business may provide an alternative opt-out link in accordance with section 7015. The business shall still post a notice of right to limit in accordance with these regulations.
- (e) A business that uses or discloses a consumer’s sensitive personal information for purposes other than those specified in section 7027, subsection (l), shall provide the notice of right to limit to consumers as follows:
 - (1) A business shall post the notice of right to limit on the internet webpage to which the consumer is directed after clicking on the “Limit the Use of My Sensitive Personal Information” link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business’s privacy policy that contains the same information. If clicking on the “Limit the Use of My Sensitive Personal Information” link immediately effectuates the consumer’s right to limit, the business shall provide the notice within its privacy policy.
 - (2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to limit. That method shall comply with the requirements set forth in section 7003.
 - (3) A business shall also provide the notice of right to limit in the same manner in which it collects the sensitive personal information that it uses or discloses for purposes other than those specified in section 7027, subsection (l). Illustrative examples follow:
 - (A) A business that uses or discloses sensitive personal information that it collected in the course of interacting with consumers offline, such as in a brick-and-mortar store, for purposes other than those specified in section 7027, subsection (l), shall also provide notice through an offline method, e.g., on the paper forms that collect the sensitive personal information or by posting signage in the area where the sensitive personal information is collected directing consumers to where the notice can be found online.
 - (B) A business that uses or discloses sensitive personal information that it collects over the phone for purposes other than those specified in section 7027, subsection (l), shall provide notice orally during the call when the sensitive personal information is collected.
 - (C) A business that uses or discloses sensitive personal information that it collects through a connected device (e.g., smart television or smart watch) for purposes other than those specified in section 7027, subsection (l), shall provide notice in a manner that ensures that the consumer will encounter the notice while using the device.
 - (D) A business that uses or discloses sensitive personal information that it collects in augmented or virtual reality, such as through gaming devices or mobile applications, for purposes other than those specified in section 7027, subsection

(l), shall provide notice in a manner that ensures that the consumer will encounter the notice while in the augmented or virtual reality environment.

(f) A business shall include the following in its notice of right to limit:

(1) A description of the consumer's right to limit; and

(2) Instruction on how the consumer can submit a request to limit. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to limit online, as required by section 7027, subsection (b)(1). If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to limit.

(g) A business does not need to provide a notice of right to limit or the "Limit the Use of My Sensitive Personal Information" link if it does both of the following:

(1) It only uses and discloses sensitive personal information that it collected about the consumer for the purposes specified in section 7027, subsection (l).

(2) It states in its privacy policy that it does not use or disclose sensitive personal information for any purpose other than what is specified in section 7027, subsection (l).

(h) A business shall not use or disclose sensitive personal information it collected during the time the business did not have a notice of right to limit posted for purposes other than those specified in section 7027, subsection (l), unless it obtains the consent of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.121, 1798.135 and 1798.185, Civil Code.

§ 7015. Alternative Opt-Out Link.

(a) The purpose of the alternative opt-out link is to provide businesses the option of providing consumers with a single, clearly-labeled link that allows consumers to easily exercise both their right to opt-out of sale/sharing and right to limit, instead of posting the two separate "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links. The alternative opt-out link shall direct the consumer to a webpage that would inform them of both their right to opt-out of sale/sharing and right to limit and provide them with the opportunity to exercise both rights.

(b) A business that chooses to use an alternative opt-out link shall title the link, "Your Privacy Choices" or "Your California Privacy Choices," and shall include the following opt-out icon to the right or left of 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 homepages. The icon shall be approximately the same size as any other icons used by the business on its webpage.



(c) The alternative opt-out link shall direct the consumer to a webpage that includes the following information:

- (1) A description of the consumer's right to opt-out of sale/sharing and right to limit, which shall comply with section 7003, subsections (a) and (b); and
- (2) The interactive form or mechanism by which the consumer can submit their request to opt-out of sale/sharing and their right to limit online. The method shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.121, 1798.135 and 1798.185, Civil Code.

§ 7016. Notice of Financial Incentive.

- (a) ~~Purpose and General Principles (1)~~ The purpose of the notice of financial incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a notice of financial incentive.
- (b) The notice of financial incentive shall comply with section 7003, subsections (a) and (b).
- (c) ~~(2)~~ The notice of financial incentive shall be ~~designed and presented in a way that is easy to read and understandable to consumers. The notice shall:~~
 - ~~(A) Use plain, straightforward language and avoid technical or legal jargon.~~
 - ~~(B) Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.~~
 - ~~(C) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.~~
 - ~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.~~
 - ~~(E) Be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference. (3)~~ If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link that takes the consumer directly to the specific section of a business's privacy policy that contains the information required in subsection (bd).
- (d) ~~(b)~~ A business shall include the following in its notice of financial incentive:
 - (1) A succinct summary of the financial incentive or price or service difference offered;

- (2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;
- (3) How the consumer can opt-in to the financial incentive or price or service difference;
- (4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
- (5) An explanation of how the ~~financial incentive or~~ price or service difference is reasonably related to the value of the consumer's data, including:
 - (A) A good-faith estimate of the value of the consumer's data that forms the basis for offering the ~~financial incentive or~~ price or service difference; and
 - (B) A description of the method(s) the business used to calculate the value of the consumer's data.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code.

ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

§ 7020. Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know ~~and Requests to Delete.~~

- (a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to delete, requests to correct, and requests to know. ~~All other businesses shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.~~
- (b) A business that does not fit within subsection (a) shall provide two or more designated methods for submitting requests to delete, requests to correct, and requests to know. One of those methods must be a toll-free telephone number. If the business maintains an internet website, one of the methods for submitting these requests shall be through its website, such as through a webform. Other ~~Acceptable~~ methods for submitting ~~these~~ requests to delete, requests to correct, and requests to know may include, but are not limited to, ~~a toll-free phone number, a link or form available online through a business's website,~~ a designated email address, a form submitted in person, and a form submitted through the mail.
- (c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to delete, requests to correct, and requests to know ~~and requests to delete~~. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the

consumer to complete and submit an online form, or a telephone with which the consumer can call the business's toll-free number.

- (d) A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted provided that the business otherwise complies with section 7004.
- (e) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:
 - (1) Treat the request as if it had been submitted in accordance with the business's designated manner, or
 - (2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

§ 7021. Timelines for Responding to Requests to Delete, Requests to Correct, and Requests to Know ~~and Requests to Delete.~~

- (a) No later than 10 business days after ~~Upon~~ receiving a request to delete, request to correct, or request to know ~~or a request to delete~~, a business shall confirm receipt of the request ~~within 10 business days~~ and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.
- (b) Businesses shall respond to a request to delete, request to correct, and request to know ~~and requests to delete within~~ no later than 45 calendar days after it receives the request. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

§ 7022. Requests to Delete.

- (a) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.
- (b) A business shall comply with a consumer's request to delete their personal information by:
 - (1) Permanently and completely erasing the personal information ~~on~~ from its existing systems ~~with the exception of~~ archived or back-up systems; ~~(2) D.~~ deidentifying the personal information; ~~(3) A.~~ or aggregating the consumer information;
 - (2) Notifying the business's service providers or contractors to delete from their records the consumer's personal information obtained in the course of providing services; and
 - (3) Notifying all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effort.
- (c) A service provider or contractor shall, upon notification by the business, comply with the consumer's request to delete their personal information by:
 - (1) Permanently and completely erasing the personal information from its existing systems except archived or back-up systems, deidentifying the personal information, or aggregating the consumer information;
 - (2) To the extent that an exception applies to the deletion of personal information, deleting the consumer's personal information that is not subject to the exception and refraining from using the consumer's personal information retained for any purpose other than the purpose provided for by that exception;
 - (3) Notifying any of its own service providers or contractors to delete from their records in the same manner the consumer's personal information obtained in the course of providing services; and
 - (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.

- (d) ~~(e)~~ If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.
- (e) ~~(d)~~ In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request. ~~(e) If the business complies with the consumer's request, †~~The business shall also inform the consumer that it will maintain a record of the request as required by section ~~7030-7101~~, subsection ~~(b)(a)~~. A business, service provider, contractor, or third party may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from ~~the business's~~ its records.
- (f) In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following:
- (1) ~~Inform the consumer that it will not comply with the consumer's request and describe~~ Provide to the consumer a detailed explanation of the basis for the denial, including any conflict with federal or state law, ~~or~~ exception to the CCPA, or factual basis for contending that compliance would be impossible or involve disproportionate effect, unless prohibited from doing so by law;
 - (2) Delete the consumer's personal information that is not subject to the exception; ~~and~~
 - (3) Not use the consumer's personal information retained for any other purpose than provided for by that exception; and
 - (4) Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception.
- (g) If a business that denies a consumer's request to delete sells personal information and the consumer has not already made a request to opt-out of sale/sharing, the business shall ask the consumer if they would like to opt-out of the sale or sharing of their personal information and shall include either the contents of, or a link to, the notice of right to opt-out of sale/sharing in accordance with section 7013.
- (h) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information as long as ~~only if a global~~ a single option to delete all personal information is also offered and more prominently presented than the other choices. A business that provides consumers the ability to delete select categories of

personal information (e.g., purchase history, browsing history, voice recordings) in other contexts, however, must inform consumers of their ability to do so and direct them to how they can do so.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections ~~1798.100~~, 1798.105, ~~1798.110~~, ~~1798.115~~, 1798.130 and 1798.185, Civil Code.

§ 7023. Requests to Correct.

- (a) For requests to correct, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to correct. The business shall inform the requestor that their identity cannot be verified.
- (b) In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer's request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.
 - (1) Considering the totality of the circumstances includes, but is not limited to, considering:
 - (A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).
 - (B) How the business obtained the contested information.
 - (C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).
 - (2) If the business is not the source of the personal information and has no documentation to support of the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.
- (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. 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.
 - (1) Business L maintains personal information about consumers that it receives from data brokers on a regular basis. Business L generally refreshes the personal information it maintains about consumers whenever it receives an update from a data broker. Business L receives a request to correct from a consumer and determines that the

information is inaccurate. To comply with the consumer's request, Business L corrects the inaccurate information in its system and ensures that the corrected personal information is not overridden by inaccurate personal information subsequently received from the data broker.

- (2) Business M stores personal information about consumers on archived or backup systems. Business M receives a request to correct from a consumer, determines that the information is inaccurate, and makes the necessary corrections within its active system. Business M delays compliance with the consumer's request to correct with respect to data stored on the archived or backup system until the archived or backup system relating to the personal information at issue is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.

(d) Documentation.

- (1) A business shall accept, review, and consider any documentation that the consumer provides in connection with their right to correct whether provided voluntarily or as required by the business.
- (2) A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following:
 - (A) The nature of the personal information at issue (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).
 - (B) The nature of the documentation upon which the business considers the personal information to be accurate (e.g., whether the documentation is from a trusted source, whether the documentation is verifiable, etc.)
 - (C) The purpose for which the business collects, maintains, or uses the personal information. For example, if the personal information is essential to the functioning of the business, the business may require more documentation.
 - (D) The impact on the consumer. For example, if the personal information has a high impact on the consumer, the business may require less documentation.
- (3) Any documentation provided by the consumer in connection with their request to correct shall only be used and/or maintained by the business for the purpose of correcting the consumer's personal information and to comply with the record-keeping obligations under section 7101.
- (4) The business shall implement and maintain reasonable security procedures and practices in maintaining any documentation relating to the consumer's request to correct.

- (e) A business may delete the contested personal information as an alternative to correcting the information if the deletion of the personal information does not negatively impact the

consumer, or the consumer consents to the deletion. For example, if deleting instead of correcting inaccurate personal information would make it harder for the consumer to obtain a job, housing, credit, education, or other type of opportunity, the business shall process the request to correct or obtain the consumer's consent to delete the information.

- (f) In responding to a request to correct, a business shall inform the consumer whether or not it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following:
- (1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effect.
 - (2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.
 - (3) Inform the consumer that, upon the consumer's request, it will note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer. The business does not have to provide this option for requests that are fraudulent or abusive.
 - (4) If a business denies a consumer's request to correct personal information collected and analyzed concerning a consumer's health, the business shall also inform the consumer that they may provide a written statement to the business to be made part of the consumer's record per Civil Code section 1798.185, subdivision (a)(8)(D). The business shall explain to the consumer that the written statement is limited to 250 words per alleged inaccurate piece of personal information and shall include that the consumer must request that the statement be made part of the consumer's record. Upon receipt of such a statement, the business shall include it with the consumer's record and make it available to any person with whom it discloses, shares, or sells the personal information that is the subject of the request to correct.
 - (5) If the personal information at issue can be deleted pursuant to a request to delete, inform the consumer that they can make a request to delete the personal information and provide instructions on how the consumer can make a request to delete.
- (g) A business may deny a consumer's request to correct if the business has denied the consumer's request to correct the same alleged inaccuracy within the past six months of receiving the request. However, the business must treat the request to correct as new if the consumer provides new or additional documentation to prove that the information at issue is inaccurate.
- (h) A business may deny a request to correct if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. The business shall inform the

requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive.

- (i) Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business shall provide the consumer with the name of the source from which the business received the alleged inaccurate information.
- (j) Upon request, a business shall disclose all the specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.106, 1798.130 1798.185, and 1798.81.5, Civil Code.

§ 7024. Requests to Know.

- (a) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (b).
- (b) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.
- (c) In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:
 - (1) The business does not maintain the personal information in a searchable or reasonably accessible format;
 - (2) The business maintains the personal information solely for legal or compliance purposes;
 - (3) The business does not sell the personal information and does not use it for any commercial purpose; and

- (4) The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.
- (d) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.
- (e) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.
- (f) A business shall use reasonable security measures when transmitting personal information to the consumer.
- (g) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.
- (h) In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer on or after January 1, 2022, including beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort. That information shall include any personal information that the business's service providers or contractors obtained as a result of providing services to the business. If a business claims that providing personal information beyond the 12-month period would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort. ~~Unless otherwise specified by the business to cover a longer period of time, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request.~~
- (i) A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to know, including by providing the business the consumer's

personal information it has in its possession that it obtained as a result of providing services to the business.

- (j) ~~(i)~~ In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.
- (k) ~~(j)~~ In responding to a verified request to know categories of personal information, the business shall provide:
- (1) The categories of personal information the business has collected about the consumer ~~in the preceding 12 months;~~
 - (2) The categories of sources from which the personal information was collected;
 - (3) The business or commercial purpose for which it collected or sold the personal information;
 - (4) The categories of third parties with whom the business shares personal information;
 - (5) The categories of personal information that the business sold ~~in the preceding 12 months,~~ and for each category identified, the categories of third parties to whom it sold that particular category of personal information; and
 - (6) The categories of personal information that the business disclosed for a business purpose ~~in the preceding 12 months,~~ and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.
- (l) ~~(k)~~ A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections ~~1798.100, 1798.105,~~ 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

§ 7025. Opt-Out Preference Signals.

- (a) The purpose of an opt-out preference signal is to provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing. Through an opt-out preference signal, a consumer can opt out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business.

(b) A business 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 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.

(c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

- (1) The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device, and, if known, for the consumer.
- (2) The business shall not require a consumer to provide additional information beyond what is necessary to send the signal. However, a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer's request to opt-out of sale/sharing. For example, a business may give the consumer the option to provide information that identifies the consumer so that the request to opt-out of sale/sharing can apply to offline sale or sharing of personal information. Any information provided by the consumer shall not be used, disclosed, or retained for any purpose other than processing the request to opt-out of sale/sharing.
- (3) 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).
- (4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business shall notify the consumer that processing the opt-out preference signal would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the consumer does not affirm their

intent to withdraw, 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).

- (5) A business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.
- (6) The business should display whether or not it has processed the consumer's opt-out preference signal. For example, the business may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.
- (7) Illustrative examples follow.
 - (A) Caleb visits Business N's website using a browser with an opt-out preference signal enabled. Business N collects and shares Caleb's browser identifier for cross-contextual advertising, but Business N does not know Caleb's identity because he is not logged into his account. Upon receiving the opt-out preference signal, Business N shall stop selling and sharing 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.
 - (B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise.
 - (C) Noelle revisits Business O's website at a later time using a different browser that does not have the opt-out preference signal enabled. Business O knows that it is Noelle because she is logged into her account. Business O shall not interpret the absence of the opt-out preference signal as consent to opt-in to the sale of personal information.

- (D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits to marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal, but must notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.
- (E) Ramona clears her cookies and revisits Business P's website with the opt-out preference signal enabled. Business P no longer knows that it is Ramona visiting its website. Business P shall honor Ramona's opt-out preference signal as it pertains to her browser or device.
- (d) The business and the platform, technology, or mechanism that sends the opt-out preference signal shall not use, disclose, or retain any personal information collected from the consumer in connection with the sending or processing the request to opt-out of sale/sharing for any purpose other than sending or processing the opt-out preference signal.
- (e) Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt-out preference signals and providing the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or an alternate opt-out link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or an alternate opt-out link. It does not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner. If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g) of this regulation, then it may, but is not required to, provide the above-referenced links.
- (f) Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not:
- (1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal.
 - (2) Change the consumer's experience with the product or service offered by the business. For example, the consumer who uses an opt-out preference signal shall have the same experience with regard to how the business's product or service functions compared to a consumer who does not use an opt-out preference signal.

- (3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. A business's display of whether or not the consumer visiting their website has opted out of the sale or sharing their personal information, as required by subsection (c)(2), shall not be in violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to the business's sale or sharing of the consumer's personal information provided that it complies with subsections (f)(1) through (3).
- (g) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the "Do Not Sell or Share My Personal Information" link or an alternate opt-out link if it meets the following additional requirements:
- (1) Process the opt-out preference signal in a frictionless manner in accordance with the CCPA and these regulations.
 - (2) Includes in its privacy policy the following information:
 - (A) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business;
 - (B) A statement that the business processes opt-out preference signals in a frictionless manner;
 - (C) Information on how consumers can implement opt-out preference signals for the business to process in frictionless manner;
 - (D) Instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.
 - (3) Allows the opt-out preference signal to fully effectuate the consumer's request to opt-out of sale/sharing. For example, if the business sells or shares personal information offline and needs additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales or sharing of personal information, then the business has not fully effectuated the consumer's request to opt-out of sale/sharing. Illustrative examples follow.
 - (A) Business Q collects consumers' online browsing history and shares it with third parties for cross-contextual advertising purposes. Business Q also sells consumers' personal information offline to marketing partners. Business Q cannot fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1) because a consumer's opt-out preference signal would only apply to Business S's online sharing of personal information about the consumer's browser or device; the consumer's opt-out preference signal would not apply to Business S's offline selling of the consumer's information because Business S could not apply it to the offline selling without additional information provided by the consumer, i.e., the logging into an account.

(B) Business R only sells and shares personal information online for cross-contextual advertising purposes. Business R may use the exception set forth in Civil Code section 1798.135, subdivision (b)(1) and not post the “Do Not Sell or Share My Personal Information” link because a consumer using an opt-out preference signal would fully effectuate their right to opt-out of the sale or sharing of their personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7026. Requests to Opt-Out of Sale/Sharing.

(a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. ~~including an interactive form accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information.~~ (b) A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the ~~sells~~ personal information that it sells to or shares with third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

- (1) ~~(c) If a~~ A business that collects personal information from consumers online, ~~the business~~ shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and through an interactive form accessible via the “Do Not Sell My Personal Information” link, alternative opt-out link, or the business’s privacy policy. ~~treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer. (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information. (2) If a global privacy control conflicts with a consumer’s existing business-specific privacy setting or their participation in a business’s financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.~~
- (2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out of sale/sharing in addition to the opt-out preference signal.

- (3) Other methods for submitting requests to opt-out of the sale/sharing include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.
- (4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.
- (b) ~~(h)~~ A business's methods for submitting requests to opt-out of sale/sharing shall be easy for consumers to execute, and shall require minimal steps, and shall comply with section 7004 to allow the consumer to opt out. A business shall not use a method is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt out. Illustrative examples follow:
- (1) ~~The business's process for submitting a request to opt out shall not require more steps than that business's process for a consumer to opt in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt in to completion of the request.~~
- (2) ~~A business shall not use confusing language, such as double negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt out.~~
- (3) ~~Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt out before confirming their request.~~
- (4) ~~The business's process for submitting a request to opt out shall not require the consumer to provide personal information that is not necessary to implement the request.~~
- (5) ~~Upon clicking the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt out.~~
- (c) A business shall not require a consumer submitting a request to opt-out of sale/sharing to create an account or provide additional information beyond what is necessary to direct the business not to sell or share the consumer's personal information.
- (d) ~~(g)~~ A business shall not require request to opt out need not be a verifiable consumer request for a request to opt-out of sale/sharing. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information shall cease to be sold or shared by the business. However, to the extent

that the business can comply with a request to opt-out of sale/sharing without additional information, it shall do so.

- (e) If a business, ~~however,~~ has a good-faith, reasonable, and documented belief that a request to opt-out of sale/sharing is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.
- (f) ~~(e)~~ A business shall comply with a request to opt-out of sale/sharing by:
- (1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Providing personal information to service providers or contractors does not constitute a sale or sharing of personal information. ~~If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt out and shall direct those third parties not to sell that consumer's information.~~
 - (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.
 - (3) Notifying all third parties to whom the business 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 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.
 - (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 "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.
- (g) ~~(d)~~ In responding to a request to opt-out of sale/sharing, a business may present the consumer with the choice to opt-out of the sale or sharing ~~for certain uses~~ of personal information for certain uses as long as a ~~global~~-single option to opt-out of the sale or sharing of all personal information is more prominently presented than the other choices. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

- (h) A business that responds to a request to opt-out of sale/sharing by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a notice of financial incentive that complies with section 7016 in its response. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).
- (i) ~~(f)~~ A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent cannot does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal. User-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.
- (j) Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer's request before asking a consumer who has opted out of the sale or sharing of their personal information to consent to the sale or sharing of their personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.

- (a) The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business's use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (l).
- (b) A business that uses or discloses sensitive personal information for purposes other than those set forth in subsection (l) shall provide two or more designated methods for submitting requests to limit. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the sensitive personal information that it uses for purposes other than those set forth in subsection (l), available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to limit. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

- (1) A business that collects sensitive personal information from consumers online shall, at a minimum, allow consumers to submit requests to limit through an interactive form accessible via the "Limit the Use of My Sensitive Personal Information" link, alternative opt-out link, or the business's privacy policy.
 - (2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to limit in addition to the online form.
 - (3) Other methods for submitting requests to limit include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.
 - (4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to limit because cookies concern the collection of personal information and not necessarily the use and disclosure of sensitive personal information. An acceptable method for submitting requests to limit must address the specific right to limit.
- (c) A business's methods for submitting requests to limit shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.
 - (d) A business shall not require a consumer submitting a request to limit to create an account or provide additional information beyond what is necessary to direct the business to limit the use or disclosure of the consumer's sensitive personal information.
 - (e) A business shall not require a verifiable consumer request for a request to limit. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer to whom the request should be applied. However, to the extent that the business can comply with a request to limit without additional information, it shall do so.
 - (f) If a business has a good-faith, reasonable, and documented belief that a request to limit is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.
 - (g) A business shall comply with a request to limit by:
 - (1) Ceasing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (l) as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.
 - (2) Notifying all the business's service providers or contractors that use or disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (l) that the consumer has made a request to limit and instructing them to comply with the consumer's request to limit within the same time frame.

- (3) Notifying all third parties to whom the business has disclosed or made available the consumer's sensitive personal for purposes other than those set forth in subsection (1), after the consumer submitted their request and before the business complied with that request, that the consumer has made a request to limit and direct them 1) to comply with the consumer's request and 2) forward the request to any other person with whom the person has disclosed or shared the sensitive personal information during that time period.
- (4) Notifying all third parties to whom the business makes sensitive personal information available for purposes other than those set forth in subsection (1), including businesses authorized to collect sensitive personal information or controlling the collection of sensitive personal information through the business's premises, that the consumer has made a request to limit and directing them 1) to comply with the consumer's request and 2) forward the request to any other person with whom the third party has disclosed or shared the sensitive personal information during that time period. In accordance with section 7052, subsection (b), those third parties and other persons shall no longer retain, use, or disclose the sensitive personal information for purposes other than those set forth in subsection (1).
- (5) Providing a means by which the consumer can confirm that their request to limit has been processed by the business. For example, the business may display through a toggle or radio button that the consumer has limited the business's use and sale of their sensitive personal information.
- (h) In responding to a request to limit, a business may present the consumer with the choice to allow specific uses for the sensitive personal information as long as a single option to limit the use of the personal information is more prominently presented than the other choices.
- (i) A consumer may use an authorized agent to submit a request to limit on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.
- (j) A business that responds to a request to limit by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a notice of financial incentive that complies with section 7016 in its response.
- (k) Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer's request to limit is received before asking a consumer who has exercised their right to limit to consent to the use or disclosure of their sensitive personal information for purposes other than those set forth in subsection (1).
- (l) The purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes is not required to post a notice of right to limit.

- (1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.
- (2) To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose. For example, a business may disclose a consumer's log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer's account.
- (3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose. For example, a business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.
- (4) To ensure the physical safety of natural persons, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose. For example, a business may disclose a consumer's geolocation information to law enforcement to investigate an alleged kidnapping.
- (5) For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business. For example, a business that sells religious books can use information about its customers' religious beliefs to serve contextual advertising for other kinds of religious merchandise within its store or on its website, so long as the business does not use the sensitive personal information to create a profile about an individual consumer or disclose consumers' religious beliefs to third parties.
- (6) To perform services on behalf of the business, such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.
- (7) To verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business. For example, a car rental business

may use a consumer's driver's license for the purpose of testing that its internal text recognition software accurately captures license information used in car rental transactions.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.121, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7028. Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information.

- (a) Requests to opt-in to ~~the sale/sharing~~ of personal information and requests to opt-in to the use and disclosure of sensitive personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.
- (b) If a consumer who has opted-out of the sale or sharing of their personal information initiates a transaction or attempts to use a product or service that requires the sale or sharing of their personal information, ~~a the~~ business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can provide consent to opt-in to the sale of sharing of their personal information. The business shall comply with section 7004 when obtaining the consumer's consent.
- (c) If a consumer who has exercised their right to limit initiates a transaction or attempts to use a product or service that requires the use or disclosure of sensitive personal information for purposes other than those set forth in subsection (1), the business may inform the consumer that the transaction, product, or service requires the use or disclosure of sensitive personal information for additional purposes and provide instructions on how the consumer may provide consent to use or disclose their sensitive personal information for those additional purposes. The business shall comply with section 7004 when obtaining the consumer's consent.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

~~§ 7031 Requests to Know or Delete Household Information.~~

- ~~(a) Where a household does not have a password protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to delete household personal information unless all of the following conditions are satisfied:~~
 - ~~(1) All consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information;~~
 - ~~(2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 7062; and~~

- ~~(3) The business verifies that each member making the request is currently a member of the household.~~
- ~~(b) Where a consumer has a password protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance with these regulations.~~
- ~~(c) If a member of a household is a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 7070.~~

~~Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140 and 1798.185, Civil Code.~~

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

§ 7050. ~~§ 7051.~~ Service Providers and Contractors.

- (a) A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a “service provider” or “contractor” under the CCPA and these regulations, shall be deemed a service provider or contractor with regard to that person or organization for purposes of the CCPA and these regulations. For example, a cloud service provider that provides services to a non-profit organization and meets the requirements and obligations of a service provider under the CCPA and these regulations, i.e., has a valid service provider contract in place, etc., shall be considered a service provider even though it is providing services to a non-business.
- ~~(b) To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business's behalf, and the second entity would otherwise meet the requirements and obligations of a “service provider” under the CCPA and these regulations, the second entity shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.~~
- ~~(b)~~ (e) A service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except:
- (1) To process or maintain personal information on behalf of the business that provided the personal information or ~~directed~~ authorized the service provider or contractor to collect the personal information.
 - (2) For the specific business purpose(s) and service(s) set forth in, and in compliance with the written contract for services required by the CCPA and these regulations.
 - (3) (2) To retain and employ another service provider or contractor as a subcontractor, where the subcontractor meets the requirements for a service provider or contractor under the CCPA and these regulations.

- (4) ~~(3)~~ For internal use by the service provider or contractor to build or improve the quality of its services, provided that the service provider or contractor ~~use~~ does not use the personal information to perform services on behalf of another person ~~include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;~~ Illustrative examples follow.
- (A) An email marketing service provider can send emails on a business's behalf using the business's customer email list. The service provider could analyze those customers' interactions with the marketing emails to improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to send marketing emails on behalf of another business.
- (B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.
- (5) ~~(4)~~ To detect data security incidents or protect against malicious, deceptive, fraudulent or illegal activity ~~or~~
- (6) ~~(5)~~ For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(~~7~~4).
- (c) A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but those services shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or from its own interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor. Illustrative examples follow.
- (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). However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them.

(2) Business T, a company that sells cookware, hires an advertising company as a service provider for the purpose of advertising its services. The advertising agency can serve Business T by providing contextual advertising services, such as placing advertisements for Business T's products on websites that post recipes and other cooking tips.

~~(d) A service provider shall not sell data on behalf of a business when a consumer has opted out of the sale of their personal information with the business.~~

~~(d)~~ (e) If a service provider or contractor receives a request to know or a request to delete request made pursuant to the CCPA directly from a the consumer, the service provider or contractor shall either act on behalf of the business in accordance with the business's instructions for responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider or contractor.

~~(e)~~ (f) A service provider or contractor that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider or contractor.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7051. Contract Requirements for Service Providers and Contractors.

(a) The contract required by the CCPA for service providers and contractors shall:

- (1) Prohibit the service provider or contractor from selling or sharing personal information it receives from, or on behalf of, the business.
- (2) Identify the specific business purpose(s) and service(s) for which the service provider or contractor is processing personal information on behalf of the business and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified business purpose(s) set forth within the contract. The business purpose or service shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.
- (3) 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).
- (4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any commercial purpose other than the business purposes specified in the contract, including in the servicing of a different business, unless expressly permitted by the CCPA or these regulations.

- (5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information received from, or on behalf of, the business with personal information that it received from another source unless expressly permitted by the CCPA or these regulations.
- (6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including providing the same level of privacy protection as required by businesses by, for example, cooperating with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.
- (7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it received from, or on behalf of, the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular assessments, audits, or other technical and operational testing at least once every 12 months.
- (8) Require the service provider or contractor to notify the business no later than five business days after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.
- (9) Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider's or contractor's unauthorized use of personal information. For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.
- (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.
- (b) A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and these regulations, including subsection (a).
- (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.

- (d) A service provider or contractor shall comply with the terms of the contract required by the CCPA and these regulations.
- (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 nor exercises its rights to 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.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7052. Third Parties.

- (a) A third party shall comply with a consumer's request to delete or request to opt-out of sale/sharing forwarded to them from a business that provided, made available, or authorized the collection of the consumer's personal information. The third party shall comply with the request in the same way a business is required to comply with the request under sections 7022, subsection (b), and 7026, subsection (f). The third party shall no longer retain, use, or disclose the personal information unless the third party becomes a service provider or contractor that complies with the CCPA and these regulations.
- (b) A third party shall comply with a consumer's request to limit forwarded to them from a business that provided, made available, or authorized the collection of the consumer's sensitive personal information for purposes other than those set forth in section 7027, subsection (l). The third party shall comply with the request in the same way a business is required to comply with the request under section 7027, subsection (g). The third party shall no longer retain, use, or disclose the sensitive personal information for purposes other than those set forth in subsection (l).
- (c) A third party that collects personal information from a consumer online (e.g., through a first party's website) and receives an opt-out preference signal shall recognize the signal as a valid request to opt-out of sale/sharing and shall not retain, use, or disclose that personal information unless informed by the business that the consumer has consented to the sale or sharing of their personal information or the third party becomes a service provider or contractor that complies with the CCPA and these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7053. Contract Requirements for Third Parties.

- (a) A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:
- (1) Identifies the limited and specified purpose(s) for which the personal information is sold or disclosed. The purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.
 - (2) Specifies that the business is disclosing the personal information to the third party only for the limited and specified purposes set forth within the contract and requires the third party to only use it for those limited and specified purposes.
 - (3) Requires the third party to comply with all applicable sections of the CCPA and these regulations, including providing the same level of privacy protection as required by businesses by, for example, only collecting and using personal information for purposes an average consumer would reasonably expect or other disclosed purposes compatible with the context in which it was collected, complying with a consumer's request to opt-out of sale/sharing forwarded to it by a first party business, providing the required disclosures identified in section 7010, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.
 - (4) Grants the business the right to take reasonable and appropriate steps to ensure that the third party uses the personal information that it received from, or on behalf of the business, in a manner consistent with the business's obligations under the CCPA and these regulations. For example, the business may require the third party to attest to their compliance with subsection (a)(3).
 - (5) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information. For example, the business may require the third party to provide documentation that verifies that they no longer retains or uses the personal information of consumers who have had their request to opt-out of sale/sharing forwarded to them by the first party business.
 - (6) Requires the third party to notify the business no later than five business days after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.
- (b) A business that authorizes a third party to collect personal information from a consumer through its website either on behalf of the business or for the third party's own purposes, shall contractually require the third party to check for and comply with a consumer's opt-out

preference signal unless informed by the business that the consumer has consented to the sale or sharing of their personal information.

- (c) A third party that does not have a contract that complies with subsection (a) shall not collect, use, process, retain, sell, or share the personal information received from the business.
- (d) A third party shall comply with the terms of the contract required by the CCPA and these regulations.
- (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 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.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

ARTICLE 5. VERIFICATION OF REQUESTS

§ 7060. General Rules Regarding Verification.

- (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to delete, request to correct, or request to know is the consumer about whom the business has collected information.
- (b) A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing or to make a request to limit. A business may ask the consumer for information necessary to complete the request; however, it shall not be burdensome on the consumer. For example, a business may ask the consumer for their name, but it shall not require the consumer to take a picture of themselves with their driver's license.
- (c) ~~(b)~~ In determining the method by which the business will verify the consumer's identity, the business shall:
 - (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.
 - (2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.
 - (3) Consider the following factors:

- (A) The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive ~~or valuable~~ personal information shall warrant a more stringent verification process. ~~The types of personal information identified in Civil Code section 1798.81.5, subdivision (d), shall be considered presumptively sensitive;~~
 - (B) The risk of harm to the consumer posed by any unauthorized ~~access or deletion,~~ correction, or access. A greater risk of harm to the consumer by unauthorized ~~access or deletion,~~ correction, or access shall warrant a more stringent verification process.;
 - (C) The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be.;
 - (D) Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.;
 - (E) The manner in which the business interacts with the consumer. ~~;~~ **and**
 - (F) Available technology for verification.
- (d) ~~(e)~~ A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101.
- (e) ~~(d)~~ A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to ~~know or request to delete,~~ request to correct, or request to know. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.
- (f) ~~(e)~~ A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized ~~access to or deletion,~~ correction, or access of a consumer's personal information.
- (g) ~~(f)~~ If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.
- (h) For requests to correct, the business shall make an effort to verify the consumer based on personal information that is not the subject of the request to correct. For example, if the

consumer is contending that the business has the wrong address for the consumer, the business shall not use address as a means of verifying the consumer's identity.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7061. Verification for Password-Protected Accounts.

- (a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 7060. The business shall also require a consumer to re-authenticate themselves before ~~disclosing or deleting, correcting, or disclosing~~ the consumer's data.
- (b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request ~~to know or request to delete, request to correct, or request to know~~ until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 7062 to further verify the identity of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

§ 7062. Verification for Non-Accountholders.

- (a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 7060.
- (b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.
- (c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.
- (d) A business's compliance with a request to delete ~~or a request to correct~~ may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of

certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion or correction. For example, the deletion of family photographs or the correction of contact information may require a reasonably high degree of certainty, while the deletion of browsing history or correction of the spelling of a name may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations.

(e) Illustrative examples follow:

- (1) *Example 1:* If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty.
 - (2) *Example 2:* If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 7060, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.
- (f) A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations.
- (g) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update the privacy policy set forth in Civil Code section 1798.130, subdivision (a)(5).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

§ 7063. Authorized Agents.

- (a) When a consumer uses an authorized agent to submit a request ~~to know or a request to delete~~, request to correct, or a request to know, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request.

The business may also require the consumer to do either of the following:

- (1) Verify their own identity directly with the business.
- (2) Directly confirm with the business that they provided the authorized agent permission to submit the request.
- (b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130. A business shall not require a power of attorney in order for a consumer to use an authorized agent to act on their behalf.
- (c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.
- (d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

ARTICLE 6. SPECIAL RULES REGARDING CONSUMERS UNDER 16 YEARS OF AGE

§ 7070. Consumers Under 13 Years of Age.

- (a) Process for Opting-In to Sale or Sharing of Personal Information
 - (1) A business that has actual knowledge that it sells or shares the personal information of a consumer under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person ~~affirmatively authorizing~~ consenting to the sale or sharing of the personal information about the child is the parent or guardian of that child. This ~~affirmative authorization consent to the sale or sharing of personal information~~ is in addition to any verifiable parental consent required under COPPA.
 - (2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:
 - (A) Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
 - (B) Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

- (C) Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
 - (D) Having a parent or guardian connect to trained personnel via video-conference;
 - (E) Having a parent or guardian communicate in person with trained personnel; and
 - (F) Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.
- (b) When a business receives ~~an affirmative authorization~~ consent to the sale or sharing of personal information pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out of sale/sharing and of the process for doing so on behalf of their child pursuant to section 7026, subsections (a)-(f).
- (c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to ~~know or a request to delete~~ request to correct, or request to know the personal information of a child under the age of 13 is the parent or guardian of that child.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 7071. Consumers 13 to 15 Years of Age.

- (a) A business that has actual knowledge that it sells or shares the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale or sharing of their personal information, pursuant to section 7028.
- (b) When a business receives a request to opt-in to the sale or sharing of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of the right to opt-out of sale/sharing at a later date and of the process for doing so pursuant to section 7026.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 7072. Notices to Consumers Under 16 Years of Age.

- (a) A business subject to sections 7070 and/or 7071 shall include a description of the processes set forth in those sections in its privacy policy.
- (b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell or share the personal information without the ~~affirmative authorization~~ consent of consumers at least 13 years of age and less than 16 years of age, or

the ~~affirmative authorization~~ consent of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out of sale/sharing.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

ARTICLE 7. NON-DISCRIMINATION

§ 7080. Discriminatory Practices.

- (a) A ~~financial incentive or a~~ price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.
- (b) A business may offer a ~~financial incentive or~~ price or service difference that is non-discriminatory. A price or service difference is non-discriminatory if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the ~~financial incentive or~~ price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the ~~financial incentive or~~ price or service difference.
- (c) A business's denial of a consumer's request to ~~know, request to delete,~~ request to correct, request to know, or request to opt-out of sale/sharing for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.
- (d) Illustrative examples follow:
 - (1) *Example 1:* A music streaming business offers a free service as well as a premium service that costs \$5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale or sharing of their personal information, then the practice is discriminatory, unless the \$5-per-month payment is reasonably related to the value of the consumer's data to the business.
 - (2) *Example 2:* A clothing business offers a loyalty program whereby customers receive a \$5-off coupon by email after spending \$100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).
 - (3) *Example 3:* A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale /sharing of their personal information. The retailer complies with their request but no longer allows the consumer to participate in

the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

- (4) *Example 4:* An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
- (e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 7016.
- (f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (i)(3), shall not be considered a financial incentive subject to these regulations.
- (g) A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.

§ 7081. Calculating the Value of Consumer Data

- (a) A business offering a ~~financial incentive or~~ price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:
 - (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.
 - (2) The average value to the business of the sale, collection, or deletion of a consumer's data.
 - (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.
 - (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.

- (5) Expenses related to the sale, collection, or retention of consumers' personal information.
 - (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.
 - (7) Profit generated by the business from sale, collection, or retention of consumers' personal information.
 - (8) Any other practical and reasonably reliable method of calculation used in good faith.
- (b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.

ARTICLE 8. TRAINING, AND RECORD-KEEPING

§ 7100. Training.

- (a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.
- (b) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135 and 1798.185, Civil Code.

§ 7101. Record-Keeping.

- (a) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.
- (b) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.

- (c) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.
- (d) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.
- (e) Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections ~~1798.100~~, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

§ 7102. Requirements for Businesses Collecting Large Amounts of Personal Information.

- (a) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, ~~or shares, or otherwise makes~~ available for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:
 - (1) Compile the following metrics for the previous calendar year:
 - (A) ~~The number of requests to know that the business received, complied with in whole or in part, and denied; (B)~~ The number of requests to delete that the business received, complied with in whole or in part, and denied;
 - (B) The number of requests to correct that the business received, complied with in whole or in part, and denied;
 - (C) The number of requests to know that the business received, complied with in whole or in part, and denied;
 - (D) ~~(C)~~ The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied; ~~and~~
 - (E) The number of requests to limit that the business received, complied with in whole or in part, and denied; and
 - (F) ~~(D)~~ The median or mean number of days within which the business substantively responded to ~~requests to know~~, requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to ~~opt out limit~~.

- (2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.

(A) In its disclosure pursuant to subsection (a)(2), a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

- (b) A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections ~~1798.100~~, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

ARTICLE 9. INVESTIGATIONS AND ENFORCEMENT

§ 7300. Sworn Complaints Filed with the Agency.

- (a) Requirements for filing a sworn complaint. Sworn complaints may be filed with the Enforcement Division via the electronic complaint system available on the Agency's website at <https://cppa.ca.gov/> or submitted in person or by mail to the Agency at the following address:

California Privacy Protection Agency
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

A complaint must:

- (1) Identify the business, service provider, contractor, or person who allegedly violated the CCPA;
- (2) State the facts that support each alleged violation and include any documents or other evidence supporting this conclusion;
- (3) Authorize the alleged violator and Agency to communicate regarding the complaint, including disclosing the complaint and any information relating to the complaint;
- (4) Include the name and current contact information of the complainant; and
- (5) Be signed and submitted under penalty of perjury.

- (b) The Enforcement Division will notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction. Duplicate complaints submitted by the same complainant may be rejected without notice.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.45, Civil Code.

§ 7301. Agency Initiated Investigations.

All matters that do not result from a sworn complaint, including Agency-initiated investigations, referrals from government agencies or private organizations, and nonsworn or anonymous complaints, may be opened on the Agency's initiative.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.145, Civil Code.

§ 7302. Probable Cause Proceedings.

- (a) Probable Cause. Under Civil Code section 1798.199.50, probable cause exists when the evidence supports a reasonable belief that the CCPA has been violated.
- (b) Probable Cause Notice. The Enforcement Division will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50.
- (c) Probable Cause Proceeding.
- (1) The proceeding shall be closed to the public unless the alleged violator files, at least 10 business days before the proceeding, a written request for a public proceeding. If the proceeding is not open to the public, then the proceeding may be conducted in whole or in part by telephone or videoconference.
 - (2) Agency staff shall conduct the proceeding informally. Only the alleged violator(s), their legal counsel, and Enforcement Division staff shall have the right to participate at the proceeding. Agency staff shall determine whether there is probable cause based on the probable cause notice and any information or arguments presented at the probable cause proceeding by the parties.
 - (3) If the alleged violator(s) fails to participate or appear at the probable cause proceeding, the alleged violator(s) waives the right to further probable cause proceedings under Civil Code section 1798.199.50, and Agency staff shall determine whether there is probable cause based on the notice and any information or argument provided by the Enforcement Division.
- (d) Probable Cause Determination. Agency staff shall issue a written decision with their probable cause determination and serve it on the alleged violator electronically or by mail. The Agency's probable cause determination is final and not subject to appeal.

- (e) Notices of probable cause and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.50, Civil Code.

§ 7303. Stipulated Orders.

- (a) At any time before or during an administrative hearing and in lieu of such a hearing, the Head of Enforcement and the person who is the subject of the investigation may stipulate to the entry of an order. If a stipulation has been agreed upon and the scheduled date of the hearing is set to occur before the next Board meeting, the Enforcement Division will apply for a continuance of the hearing.
- (b) The order must be approved by the Board, which may consider the matter in closed session.
- (c) The stipulated order shall be public and have the force of an order of the Board.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.199.35 and 1798.199.55, Civil Code.

§ 7304. Agency Audits.

- (a) Scope. The Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA.
- (b) Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA. Alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.
- (c) Audits may be announced or unannounced as determined by the Agency.
- (d) Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.
- (e) Protection of Personal Information. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977, Civil Code section 1798, et seq.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.185, 1798.199.40 and 1798.199.65, Civil Code; Section 11180, Government Code.

From: **Nate Haderlie** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment - Small and Ethnic Businesses
Date: 24.08.2022 00:28:37 (+02:00)
Attachments: Small Business Response to CPPA Fiscal Statement 8-16.pdf (6 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello CPPA Board and Staff,

Thank you for the opportunity to submit comment for the upcoming Board Meeting.

Attached is a letter co-signed by 79 organizations that represent the small and ethnic businesses of California. The letter expresses concerns with the fiscal analysis of the compliance to the CCPA and CPRA regulations will have on their businesses.

Please feel free to connect with me if you have any questions.

Thank you,



Nathan Haderlie

Sr. Account Executive
[REDACTED]

[Website](#) | [Twitter](#) | [Facebook](#) | [Instagram](#)





August 23, 2022

Chair Jennifer M. Urban
California Privacy Protection Agency
2101 Arena Blvd., Sacramento, CA 95834
Sacramento, CA 95814

Dear Chair Urban,

On behalf of California's leading small and ethnic businesses, industries, and job creators, we are writing to express our concerns with the recent Economic and Fiscal Impact Statement (Statement) submitted by the California Privacy Protection Agency (CPPA). We believe the Statement is fundamentally flawed and vastly underestimates the time and direct costs associated with compliance and the potential business impacts around the frequently changing regulations. We respectfully request that you hold a hearing to fully assess the financial costs relating to the regulations and revise the analysis to consider the actual costs, job and business impacts, and alternative, less costly means to accomplish the goals of the California Privacy Rights Act.

First, the Economic and Fiscal Impact Statement contradicts the independent economic impact assessment prepared for the Office of the Attorney General which found that the total initial cost of compliance of the California Consumer Privacy Act (CCPA) for businesses in California was estimated to be \$55 billion. In stark contrast, the CPPA's recently submitted the Economic and Fiscal Impact Statement, stating its proposed regulations will have an initial compliance cost of \$128 for each of the 66,076 California businesses impacted by the newly created data privacy regulations. The difference between the two cost estimates on businesses is extremely troubling and creates an additional layer of confusion for small businesses.

Second, the proposed initial cost severely underestimates the cost and labor burden on small businesses. Our small businesses face many changes and uncertainties with these newly proposed laws and regulations and will be required to plan, implement, and evaluate its technological processes, vendor partnerships, privacy policies, among many other onerous measures required to comply with the CPPA's proposed regulations. Many businesses will be forced to hire lawyers, IT consultants, and additional staff to ensure proper compliance, manage consumer privacy requests, and prepare for cybersecurity audits and risk assessments – all of which undoubtedly exceed the estimated \$128 compliance cost and the “expected 1.5 hours in increased labor required for CCPA compliance.”

Third, the Statement determines that there will be 66,076 California businesses impacted, with 43,843 of those being small businesses. Considering that there are approximately 4.1 million small businesses in California, it is highly unlikely that only 1% will be directly affected by the regulations or indirectly by cost increases or loss of services from other businesses.

Lastly, the unrealistic cost and labor estimates call into question the competency of the regulatory process and explain the public and business confusion around the regulations.

- “A recent survey by [ESET](#) polled 625 business owners and executives to gauge the business readiness for this regulation. Nearly half (44.2%) had never heard of CCPA. Only 11.8% know if the law applies to them, and 34% are unsure if they need to change how they capture, store and process data.”
- “As of March 31, 2022, the findings uncovered that 90% of companies are not fully compliant with CCPA and CPRA Data Subject Access Request (DSAR) requirements. (Source: CYTRIO data privacy [research](#))”

It is a critical time for consumers and small business owners -- Californians face high inflation, job reductions in the tech sector, and a potential recession. We urge the CPPA to slow down and provide a realistic and thorough economic analysis that will lead to more successful regulatory program

Respectfully,

- Asian Industry Business to Business
- Associated Builders and Contractors Northern California
- Automotive Service Councils of California
- Bay Area Builders Exchange
- Beverly Hills Chamber of Commerce
- BuildOUT California
- California African American Chamber of Commerce
- California Asian Chamber of Commerce
- California Association of REALTORS
- California Autobody Association
- California Automotive Business Coalition
- California Beer & Beverage Distributors
- California Black Chamber of Commerce
- California Builders Alliance
- California Business Properties Association
- California Business Roundtable
- California Chamber of Commerce
- California Craft Brewers Association
- California Delivery Association
- California Farm Bureau Association
- California Food Producers
- California Golf Course Owners Association
- California Hispanic Chambers of Commerce
- California Manufacturers & Technology Association
- California Medical Association
- California New Car Dealers Association
- California Pool & Spa Association
- California Restaurant Association
- California Retailers Association

- California Small Business Association
- California Tire Dealers Association
- California Urban Partnership
- California's Builders Alliance
- Coalition of Labor, Agriculture, and Business
- Coalition of Small & Disabled Veteran Businesses
- Culver City Chamber of Commerce
- Danville Area Chamber of Commerce
- El Dorado County Chamber of Commerce
- Elk Grove Chamber of Commerce
- Family Business Association of California
- Flasher Barricade Association
- Folsom Chamber of Commerce
- Glendale Chamber of Commerce
- Golden Gate Business Association
- Golden Gate Restaurant Association
- Greater Arden Chamber of Commerce
- Greater Stockton Area Chamber
- Independent Automotive Professionals Association
- Latin Business Association
- Long Beach Area Chamber of Commerce
- Los Angeles County Business Federation
- Los Angeles Latino Chamber of Commerce
- National Association of Women Business Owners
- National Federation of Independent Business
- Nevada County Contractors Association
- North Coast Builders Exchange
- Orange County Business Council
- Orange County Hispanic Chamber of Commerce
- Painting & Decorating Contractors Association of Sacramento
- Placer County Contractors' Association
- Plumbing-Heating-Cooling Contractors of California
- R Street Corridor
- Rancho Cordova Chamber of Commerce
- Roofing Contractors Association of California
- Sacramento Black Chamber of Commerce
- San Juan Capistrano Chamber of Commerce
- Santa Monica Chamber of Commerce
- SCALE Health
- Slavic American Chamber of Commerce
- Small Business California
- Tech CA

- The Wine Institute
- United Chamber Advocacy Network
- United Chambers of Commerce of the San Fernando Valley
- Valley Contractors Exchange
- Valley Industry & Commerce Association
- Ventura County Contractors Association
- Western Steel Council
- Yuba Sutter Chamber of Commerce

From: **Justin Kloczko** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 24.08.2022 15:54:11 (+02:00)
Attachments: CPPAletterCW.pdf (3 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Apologies, but this is the final version of Consumer Watchdog's letter. Thank you.



California Privacy Protection Agency
 915 Capitol Mall 350 A
 Sacramento, CA 95814

Re: Comments on proposed regulations

Dear Board Members,

Consumer Watchdog writes to commend the Agency for its thorough draft regulations to implement the California Consumer Privacy Rights Act. We applaud that the rules strive to make it easier for people to take control of their data more than ever before. The regulations, drafted in response to protections California voters passed at the ballot, provide needed guidance on what can be considered a dark pattern, the kind of deceptive language and design businesses often use to extract user consent online. By detailing specific ways in which consent should be obtained that is not manipulative, the regulations help ensure businesses cannot interfere with consumer choices. Businesses must also provide a list of categories of sensitive information collected, whether personal information is sold or shared.

What follows are more detailed comments regarding a few areas of the regulations:

Connected Cars: In light of car companies collecting reams of personal data as outlined in our report, [“Connected Cars and the Threat to Your Privacy.”](#) Consumer Watchdog has urged you to draw regulations that would make clear connected car companies that track geolocation and other information cannot use or sell that data beyond a “legitimate operational use.” The regulations on use limits ensure drivers can protect their data. We applaud the Agency for rejecting car and telematics companies’ efforts to incorrectly interpret the CPRA to exempt automotive data collection from the law. The regulations require data collection and use by any business – including a business collecting data through the infotainment system in cars – be proportionate to the purpose. For example, under section 7002, a flashlight app on a person’s phone should not collect geolocation without that person’s consent because an average person would not expect the app to have to know geolocation for the function of the flashlight. Likewise, a car company that knows your location for emergency services such as a car accident should not use geolocation for purposes unrelated to safety.

Global Opt-Out/Ease of Use: We commend the regulation 7025 for making clear that companies must both display a “Do Not Share/Sell My Information” button and “Limit the Use of My Sensitive Personal Information” button on their home page, and honor a global opt-out signal. The homepage button is crucial for informing consumers who are not aware of their privacy rights. The global opt-out is critical to make privacy choices as seamless as possible for those who already know they want to exercise their rights. Requiring global privacy signals be honored by businesses is an easy, fluid way for consumers to notify all businesses of their privacy preferences. In addition, the regulations state that a business should display a message on its website as to whether it has honored a user’s preference signal. This simple notification will

protect consumers from going through additional opt-out steps if they are unsure their rights have been honored. It will also enable consumers to flag websites for enforcement by the Agency if those rights are not honored.

That many advertising and tech industry firms who see our data as a pot of gold have come out against a global opt-out, including the California Retailer's Association and the California Chamber of Commerce, says something about the importance of such mechanism for consumers. The chamber, which includes among its members major personal data recipients Google, Amazon and Facebook, insurance companies State Farm and Allstate, and big banks Wells Fargo and JP Morgan Chase, said, incorrectly, "a global opt-out is voluntary under the California Privacy Rights Act."

However, we worry about businesses making it difficult for consumers to exercise that opt-out right.

Under the proposed regulation Section 7025, it says, "a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer's request to opt-out of sale or selling." This opens the door to a lot of friction in the form of pop-ups or worse service, which goes against the intent of the law.

For example, companies may still ask for information even if "do not sell/share" is enabled. The law could be interpreted as allowing companies to ask for a name and email frequently, and consumers will get fatigued for being punished for exercising privacy rights. The ability for a business to have the so-called "last say" in this exchange over data sharing should be simply eliminated. Indeed, the Agency's regulations state, *"The path for a consumer to exercise a more privacy-protective option shall not be longer than the path to exercise a less privacy-protective option."*

15-days to Honor Opt-Out of Sale/Sharing: Under Sections 7026 and 7027, businesses have 15 days to honor a person's request to stop selling or sharing data with third-parties, as well as 15 days to limit use and disclosure of sensitive personal information. This is a massive window that threatens to upend the intent of the entire law. And the regulation is not backed up by the statutory language. The problem is once people's data is acquired it is usually sold by businesses right away, oftentimes in seconds. Once data gets out into the world, [it can get into anyone's hands](#). Even when someone opts out, personal information will still be sold because businesses are granted a two-week grace period. It will also spur companies to concentrate on using and selling data within the window, producing a Wild West effect on data selling. And even though it says a business should honor a request "as soon as feasibly possible," a business will cite 15 days as "soon as feasibly possible." Businesses should be forced to honor a person's opt-out request just as soon as they are able to sell your data, which apparently is mere seconds. Please close this gap.

Thank you for hearing our concerns and drafting the strongest privacy rules in the country on behalf of California voters. We look forward to seeing final regulations that address these issues, as well as the next round of draft rules.

Sincerely,



Justin Kloczko

From: **Jamiene a [REDACTED]**
To: **Regulations** <Regulations@cpga.ca.gov>
Subject: CPPA Public comment
Date: 24.08.2022 16:31:41 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

My name is Jamiene a [REDACTED] and I would love to share my concerns about having mine and my childrens/family personal information accessible to see and/or purchase on many platforms. I recently went through a very intense stalking case where I was victimized in Los Angeles. Mine and my childrens emails as well as social media was entirely hacked by these 2 individuals. 1/2 individuals (summer M [REDACTED]) stalked me for almost 2 years and it was made known that they first found our house address , phone numbers etc information on a website that you can buy peoples information. I spent almost 6 days opting out of numerous websites but it was an endless search and I unfortunately was not able to completely remove all of our information of all the websites. 1/2 of the individuals was arrested but justice was never served as they hired a very expensive defense attorney who defamed my character as well as sabotaged my case. I could not afford an attorney and so these people were never fully prosecuted. When they obtained my home address and phone numbers they were sending me photos of me and my kids walking into my house and we'll as numerous crank calls that to this day still exist. I have changed my number a total of 10 times but these websites continue to provide updated numbers for me and my family. It is clear and apparent that this is a severe safety concern and has caused im sure many people including myself to suffer great danger. I would love to have our information banished from any and all websites asap. I will be participating in the conference on 08/25 in hopes for justice. I just changed my number again 3 days ago because the harassment still continues. And yet again crank calls are coming in. My number to reached at is [REDACTED] Please let me know if there is anything to I can do to make a change. Thank you In advance!

Sent from my iPhone

From: **Ashlee Garrison** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 24.08.2022 11:22:35 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello, Chair and board members. My name is Ashlee Garrison and I am the owner of Social Hour With ASH, a small, minority-owned business in Walnut Creek, CA. I appreciate the opportunity to provide comments before the board today.

The regulations recently published, caused my business to quickly work to get a grip on this complex regulatory framework and make sure we understand how we will be affected. If we make a mistake, my business could be subject to costly lawsuits that will force us to close our doors.

Without online platforms, my business, would simply not exist. We cannot afford to lose such an important tool.

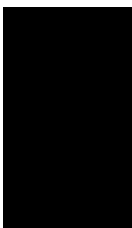
We remain committed to protecting the privacy of our customers and providing the best services we can.

However, with very little time left to comply with such complicated regulations, I am concerned how this framework will affect my business and other small, minority-owned businesses in California.

Please listen to the voices of small business owners like myself and consider the very real impact these regulations and the missed deadlines will have. Thank you.

Regards,

Ashlee Garrison



Overcome to Become - Social Hour With ASH - Ashlee Garrison

From: [REDACTED]
 To: **Regulations** <Regulations@coppa.ca.gov>
 Subject: CCPA Public Comment
 Date: 24.08.2022 11:46:26 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please enter the following comments into the Public Record regarding the

California Privacy Protection Agency, Title 11. Law Division 6. California Privacy Protection Agency

Chapter 1. California Consumer Privacy Act Regulations – Hearing date 8/24/22

Dear Honorable Members of the CPPA Committee:

I have always felt it was important in business to follow this motto: *"If you aren't at the table, then you are on the menu."*

After listening to today's zoom meeting, it feels as though this entire process has been held in a vacuum leaving out important part of the package – the business community. I certainly am an advocate for consumer rights, but I am also an advocate for fairness

and a WIN for all – the consumer, government, AND business.

I have been in business for over 40 years in California and the last 5 years have been the hardest. The pandemic was one thing but coming

out of the pandemic has been like all the government rule makers had time to get together and have zoom meetings to figure out new ways

to either make new rules or collect more fees! They didn't hold hearings and they were NOT held accountable to anyone. This proposed

rulemaking is another one of those grand ideas – or at least that is how I feel!

Effect of the Proposed Rulemaking:

I strongly disagree with the statement *"The Agency has determined that these proposed regulations are not inconsistent or incompatible*

with existing State regulations." The Agency apparently has not read nor reached out to the Bureau of Automotive Repair in their current

Write it Right regulations for the automotive repair industry. The collection of data is part of making sure the client has properly authorized the

repairs on their vehicle. There are many large corporations in our state doing business that need to comply with those regulations.

I think before the Agency establishes anymore rules, they establish a place where data companies or technology companies, who wish to operate

systems within the State of California need to go through a rigorous review process to make sure they meet ALL state standards and requirements

so, companies purchasing or using their services in the state have an assurance they are following ALL state AGENCY rules and regulations.

In other words, a CA State of APPROVAL for all IT/Data companies doing business in California. Instead of doing business in California and being the

"GOTCHA STATE".

Who believes it is only going to cost \$127.50 to comply? What was used to determine those costs? What programmer in the State of California

is going to bring a program as intrinsic as some of these are for that price? What about employee training costs and new processes? Compliance

reporting costs?

Yes, consumers have rights! Lots of consumers don't even read the existing opportunities to "opt out" and would rather scream foul! I really do not

believe this is as big of a consumer issue as it is being made but rather a few complainers that have gotten the ear of a powerful politician who wants

to be a hero! Maybe the easiest solution is just change the font size of the "opt out" or "unsubscribe" and make it a day.

Thank you for letting me offer my thoughts.

Sincerely,

Nikki Ayers

Santa Barbara, CA

From: **Buck Stoval** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: internet privacy act denied
Date: 24.08.2022 15:55:47 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

The problem I have with protecting my privacy is the websites are like a corn maze to try to find the link to the don't sell my personal data button. Many times it's pages and pages of corporate policy but no link visible.

Can you make it standardized so it's easy to find.

Recently I tried to see my personal data with T-Mobile. After sending pictures of my driver's license front and back and personal photograph the site crashed on the last item .. it kept finding a problem with my data and I would have to start all over again, forms and pictures. 45 minutes later I just gave up.

I want to know if I have a perfect driving record or if something is there that caused my rates to increase. I'm beginning to feel like a victim of the internet privacy act denied.

From: **Eric Rosenkoetter** [REDACTED]
 To: **Regulations** <Regulations@cpga.ca.gov>
 Subject: CPPA Public Comment - Receivables Management Association International
 Date: 24.08.2022 19:30:21 (+02:00)
 Attachments: RMAI Comments to CPPA NPRM 08-22-2022.pdf (13 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear CPPA:

The Receivables Management Association International appreciates this opportunity to submit the attached comments in response to the Notice of Proposed Rulemaking dated July 8, 2022.

Thank you, and please let us know if you have any questions.

Sincerely,

Maurice Wutscher LLP, General Counsel for RMAI

Eric P. Rosenkoetter
Maurice Wutscher LLP
 13785 Research Blvd., Suite 125
 Austin, Texas 78750
 Direct: [REDACTED]
 Mobile: [REDACTED]
 Email: [REDACTED]

Admitted to practice in Texas and Missouri

MauriceWutscher

ALABAMA | CALIFORNIA | FLORIDA | ILLINOIS | MASSACHUSETTS | NEW JERSEY | NEW YORK
 | OHIO | PENNSYLVANIA | TENNESSEE | TEXAS | WASHINGTON, D. C.

www.MauriceWutscher.com

CONFIDENTIALITY NOTICE: This communication (including any related attachments) may contain confidential and/or privileged material. Any unauthorized disclosure or use is prohibited. If you received this communication in error, please contact the sender immediately, and permanently delete the communication (including any related attachments) and permanently destroy any copies.

IRS CIRCULAR 230 NOTICE: To the extent that this message or any attachment concerns tax matters, it is not intended to be used and cannot be used by any taxpayer for the purpose of avoiding penalties that may be imposed by law.

MauriceWutscher
www.MauriceWutscher.com

Alabama | California | Florida | Illinois | Massachusetts | New Jersey | New York |
 Ohio | Pennsylvania | Tennessee | Texas | Washington, DC

CONFIDENTIALITY NOTICE: This communication (including any related attachments) may contain confidential and/or privileged material. Any unauthorized disclosure or use is prohibited. If you received this communication in error, please contact the sender immediately, and permanently delete the communication (including any related attachments) and permanently destroy any copies.

IRS CIRCULAR 230 NOTICE: To the extent that this message or any attachment concerns tax matters, it is not intended to be used and cannot be used by any taxpayer for the purpose of avoiding penalties that may be imposed by law.

California Privacy Protection Agency
 Attn: Brian Soublet
 2010 Arena Blvd.
 Sacramento, CA 95834



1050 Fulton Avenue #120
 Sacramento, California 95825
 916.482.2462

Sent via email: Regulations@coppa.ca.gov

August 22, 2022

Re: RMAI Comments on CCPA Proposed Regulations

Dear Mr. Soublet:

The Receivables Management Association International (“RMAI”) appreciates this opportunity to submit the following comments to the California Privacy Protection Agency (“Agency”) regarding the Proposed Regulations relating to the California Consumer Privacy Act of 2018 (“CCPA”) and California Privacy Rights Act (“CPRA”).

I. BACKGROUND

RMAI is the nonprofit trade association that represents more than 590 companies that purchase or support the purchase of performing and non-performing receivables on the secondary market. The existence of the secondary market is critical to the functioning of the primary market in which credit originators extend credit to consumers. An efficient secondary market lowers the cost of credit extended to consumers and increases the availability and diversity of such credit.

RMAI is an international leader in promoting strong and ethical business practices within the receivables management industry. RMAI requires all its member companies who are purchasing receivables on the secondary market to become certified through RMAI’s Receivables Management Certification Program (“RMCP”)¹ as a requisite for membership. The RMCP is a comprehensive and uniform source of industry standards that has been recognized by the collection industry’s federal regulator, the Bureau of Consumer Financial Protection, as “best practices.”²

RMAI supports the adoption of reasonable measures designed to protect consumer privacy. With respect to data security, RMCP certified companies are required to establish and maintain a reasonable and appropriate data security policy that includes, at a minimum, measures to ensure:

- (a) The safe and secure storage of physical and electronic Consumer Data;

¹ RMAI, *RMAI Receivables Management Certification Program*, <https://rmassociation.org/certification> (last accessed August 15, 2022).

² Consumer Financial Protection Bureau, *Small Business Review Panel for Debt Collector and Debt Buyer Rulemaking, Outline of Proposals Under Consideration*, July 28, 2016, p. 38, http://files.consumerfinance.gov/f/documents/20160727_cfbp_Outline_of_proposals.pdf (last accessed August 15, 2022).

(b) Computers and other electronic devices that have access to Consumer Data contain reasonable security measures such as updated antivirus software and firewalls;

(c) Receivables portfolios are not advertised or marketed in such a manner that would allow Consumer Data and Original Account Level Documentation to be available to or accessible by the public;

(d) If there is any offsite access to a Certified Company's network, the offsite access shall be through the use of a virtual private network "VPN" or other system that requires usernames and passwords, complex and non-intuitive passwords, recurring password changes, and multifactor authentication;

(e) The Certified Company can prevent connectivity with the network and/or remotely disable or wipe company-issued computers and electronic devices that contain Consumer Data when an employee or agent no longer has an employment/agency relationship with the company or if a device is lost or stolen;

(f) Consumer Data that is transferred to a third-party is transferred securely through the use of encryption or other secure transmission sources;

(g) An action plan has been developed and communicated with relevant employees on how to handle a data breach in accordance with applicable laws, which shall include any required disclosures of such breach;

(h) A disaster recovery plan has been developed and communicated with relevant employees on how to respond to emergencies (e.g., fire, natural disaster, etc.) that have the potential to impact the use and storage of data; and

(i) The secure and timely disposal of Consumer Data that complies with applicable laws and contractual requirements, provided that account records are maintained for at least three (3) years from the date of last collection activity.³

II. COMMENTS

Article 1. General Provisions.

§ 7001. Definitions.

"Affirmative Authorization." RMAI understands this definition was removed because "Civil Code section 1798.140, subdivision (h), now defines 'consent.'"⁴ However, the Proposed

³ RMAI Certification Standard A7, v10.

⁴ Initial Statement of Reasons ("ISR"), p. 3.

Regulations repeatedly use the phrase “explicit consent,”⁵ which is not defined. It would be helpful to have specific guidance on how “consent” and “explicit consent” differ.

“Authorized Agent.” The requirement that a business acting as an authorized agent be “registered with the Secretary of State to conduct business in California” was removed because “businesses have misinterpreted this language to mean that there is a special registry with the Attorney General’s Office for authorized agents.”⁶ If that is the reasoning, it makes more sense to provide clarification than to remove the requirement altogether. The proposed amendment opens the door for any “business entity” to act as an authorized agent even if not registered with the Secretary of State. Ostensibly, that is not the result the Agency is seeking.

“Disproportionate Effort.” RMAI appreciates the Agency’s attempt to provide greater clarity around this term that appears in Civil Code §§ 1798.105, 1798.130, and 1798.185.⁷ Nevertheless, it will be a high compliance hurdle for businesses to draft specific policies and procedures, by which they will be audited, to conform to this definition. RMAI respectfully recommends the definition be more definite.

“Household.” RMAI understands this definition was deleted “because Civil Code section 1798.140, subdivision (q), now defines ‘household.’”⁸ Unfortunately, the statutory definition omits the requirement of a group account or unique identifier, which was a commonsense requirement in the context of the CCPA and considering the purpose of the definition in the first place. RMAI suggests that the regulations clarify that in the context of the definition of “household,” “however identified” means however identified by a business, whether as sharing a group account, a unique identifier, or otherwise.

“First Party.” This definition is subjective and speculative regarding with whom a consumer “intends and expects” to interact. The term should include not only consumer-facing businesses with which the consumer intends and expects to interact as a direct response to a request for goods or services, but also consumer-facing businesses with which the consumer should reasonably foresee interacting with as a result. For example, a consumer who obtains a loan will intend and expect to interact with the lender. However, it is reasonably foreseeable, though perhaps not expected or intended, that the consumer may also interact with a third-party loan servicer, another lender if the loan is sold, or even a collection agency if the consumer defaults on the loan.

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

§ 7002(a). The term “average consumer” is a troublesome standard. RMAI requests that the Agency provide guidance on how it will define the “average” consumer when undertaking enforcement action.

⁵ §§ 7002(a), 7002(b)(1)-(b)(4).

⁶ ISR, p. 4.

⁷ ISR, p. 4.

⁸ ISR, p. 4.

§ 7002(b)(2). RMAI appreciates the useful examples provided to aid in understanding the application of the proposed regulations. However, what is “expected” or “reasonably necessary and proportionate to achieve the purpose” is subjective and may be difficult to determine. For instance, in the “Business B” example, if the facial recognition service is developed to provide the consumer with more secure access to their cloud storage, that new service is arguably related, but not necessarily expected.

§ 7002(c). RMAI believes it would be helpful if the regulations clarified how a new notice at collection should be provided to consumers, particularly in certain circumstances. For example, in the context of using previously obtained personal information for a new purpose, what if there has been no recent relationship, or if the initial collection of information did not include contact information? In those instances, a business may need to contract with a service provider to obtain up to date contact information simply to provide the notice, which could be considered contrary to the CCPA’s data minimization requirements.

§ 7003. Requirements for Disclosures and Communications to Consumers.

§ 7003(a). “Easy to read and understandable to consumers,” using “straightforward language” is an extremely subjective standard. While examples and comparisons of acceptable versus non-acceptable language would be helpful, readability statistics would provide a more objective standard.

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

§ 7004(a)(2). RMAI appreciates that the symmetry standard can be objective, i.e., number of clicks, but notes there could legitimate reasons an opt-out may require more steps. RMAI suggests that there should be an exception to the symmetry standard if a business can demonstrate that it is reasonable for its opt-out process to take more steps than the opt-in process.

§ 7004(c). This section provides: “A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, *regardless of a business’s intent*.” (emphasis added) This definition differs from that in Civil Code § 1798.140(l): “‘Dark pattern’ means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.”

The Agency argues that the statutory definition explicitly disregards “the intent of the business when creating the interface.”⁹ RMAI respectfully disagrees. The statute is silent on whether the design of an interface with the violative characteristics may be unintentional, or must be intentional. RMAI suggests that because of the subjectivity involved in determining whether a

⁹ ISR, p. 13.

dark pattern exists, the regulations should clarify that the design of a dark pattern interface must be intentional.

Article 2. Required Disclosures to Consumers.

§ 7011. Privacy Policy.

§ 7011(c)(2). This subpart requires that a business’s privacy policy notify consumers of their rights under the CCPA. However, many businesses only process personal information that is exempt from the CCPA pursuant to Cal. Civ. Code §1798.145. Accordingly, requests received will be denied with explanation, pursuant to §§ 7022(f)(1), 7923(f)(1), and 7024(e).

Informing consumers of their rights knowing that certain requests will be denied seems disingenuous and a waste of consumers’ time. Accordingly, RMAI suggests that the Agency clarify that neither the CCPA nor its regulations prohibit a business from explaining in its privacy policy that because the entity is exempt from the CCPA, or because the personal information collected, processed, sold, or disclosed by the entity is exempt, consumers’ requests to exercise their rights under the CCPA may be denied.

Article 3. Business Practices for Handling Consumer Requests

§ 7020 Methods for Submitting Requests to Delete, Requests to Correct and Requests to Know.

§ 7020(b). Businesses that operate only informational websites should not be required to accept requests to dispute or know using a webform. A survey conducted of RMAI members revealed that twenty percent (20%) operate websites that are not designed to collect information from or otherwise interact with consumers. These websites are designed as online brochures and are primarily used to advertise to the credit and collection industry. They do not engage consumers. Because the proposed regulation would apply to any business that “maintains an internet website,” regardless of whether the website collects information of consumers, it imposes an unnecessary burden.

Existing and proposed subpart (c) contemplates this very situation, noting:

A business shall consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests [to delete, requests to correct and requests to know](#) ~~and requests to delete~~.” Thus, where a business does not use a website to interact with consumers, it should not be required to provide a webform to receive requests.

One important reason not to require “webforms” and similar web-based communications channels is to protect consumer privacy. The use of web-forms as an exploit by bad actors has exploded over the past two years. In a 2020 survey published by Cybersecurity Insiders, web

server exploits were identified as a “most dangerous” malware attack vector by surveyed cybersecurity professionals.¹⁰ Those same surveyed cybersecurity professionals pointed to customer information and financial data as the data “most at risk” to such exploits.¹¹

The use of webforms to exploit sensitive non-public, private information is well documented. In 2008, criminals obtained 100 million debit and credit card numbers through a “SQL injection” into a webform on the website of Heartland Payment Systems.¹² In 2017, the Equifax data breach began through an exploit of its consumer complaint web portal.¹³

A business should exercise reasonable and appropriate measures to address data security. One measure to protect against the very type of exploit identified in the Equifax is to simply not allow consumers “methods for submitting these requests . . . through its website.” In fact, as recent as August 11, 2022, the Consumer Financial Protection Bureau issued a circular explaining that in the case of the Equifax breach, Equifax’s use of the unsecured webform portal to collect consumer complaints violated the federal Consumer Financial Protection Act’s prohibition against unfair acts and practices.¹⁴ (“Equifax violated the prohibition on unfairness. . . by using software that contained a known vulnerability and failing to patch the vulnerability for more than four months. Hackers exploited the vulnerability to steal over 140 million names, dates of birth, and SSNs, as well as millions of telephone numbers, email addresses, and physical addresses, and hundreds of thousands of credit card numbers and expiration dates.”). To address such vulnerabilities, companies are expected to “routinely update systems, software, and code (including those utilized by contractors).”¹⁵

As a result, a business may reasonably choose to secure consumer data by not using webforms or accepting non-public personal information through a web portal. A regulation designed to protect consumer privacy should not require the use of platforms proven, time and again, to have compromised the private data of millions of Americans. The proposed amendment creates an unacceptable risk for both covered entities and consumers. To be sure, even if a covered entity was to accept documents and data through a secure and carefully protected webform, consumers

¹⁰ Cybersecurity Insiders, *2020 Malware and Ransomware Report*, p. 10, publicly available at <https://static.helpsystems.com/core-security/pdfs/reports/cts-2020-malware-report-coresecurity.pdf> and archived at <https://perma.cc/UPC2-4KKU>.

¹¹ *Id.*, p. 8.

¹² *Heartland Payment Systems: Lessons Learned from a Data Breach*, Cheney, Julia S., Federal Reserve bank of Philadelphia, Payment Cards Center, (Jan 2010), pp. 2-3. Publicly available at <https://www.philadelphiafed.org/-/media/frbp/assets/consumer-finance/discussion-papers/D-2010-January-Heartland-Payment-Systems.pdf> and archived at <https://perma.cc/WB7J-VCLN>.

¹³ *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, United States Government Accountability Office, Report to Congressional Requestors, (GAO-18-559 Data Protection) (Aug. 2018), p. 10 (“The breach of an Equifax online dispute portal from May to July 2017 resulted in the compromise of records containing the PII of at least 145.5 million consumers in the U.S. and nearly 1 million consumers outside of the U.S.”). Publicly available at <https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf> and archived at <https://perma.cc/8ZMV-JQAB>.

¹⁴ “Insufficient data protection or security for sensitive consumer information,” Consumer Financial Protection Bureau Circular 2022-04 (Aug. 11, 2022), p. 4, publicly available at https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf and archived at <https://perma.cc/3TEH-6YT4>.

¹⁵ *Id.*, p. 7.

are still at risk. The Federal Bureau of Investigation reports that “spoofing” of website domains has become a common means by which cybercriminals obtain consumer information.¹⁶ “Spoofed” domains are websites made to appear like a trusted website, usually by making a slight alteration to a known URL. To be sure, the FBI identified its own domain as subject to potential spoofing.¹⁷

§ 7020(f) (Proposed). Requiring businesses subject to the federal Fair Debt Collection Practices Act (“FDCPA”), 15 USC § 1692, *et seq.*, to notify consumers of their rights to know, correct, or delete, will confuse consumers.

Businesses, including most RMAI members, that are subject to the FDCPA are required to notify consumers of the right to obtain “verification” of a debt. 15 USC § 1692g(a). A consumer can obtain verification by contacting the debt collector “in writing.” RMAI believes that requests to know and requests to correct could be seen as synonymous with a request for verification under the FDCPA, as they are requests for information the debt collector has concerning the consumer.¹⁸ It is likely that a consumer will believe that by submitting a request to know or request to correct using a 1-800 telephone number or a webform, they have exercised their validation rights under the FDCPA. This would not be the case since neither communication was made “in writing.”¹⁹

Additionally, RMAI believes that a consumer is likely to believe that a request to delete is synonymous with a demand to cease communications under § 1692c(c), which provides:

If a consumer notifies a debt collector in writing that the consumer refuses to pay a debt or that the consumer wishes the debt collector to cease further communication with the consumer, the debt collector shall not communicate further with the consumer with respect to such debt . . .

In fact, out of an abundance of caution and for the purpose of mitigating risk, a business subject to the FDCPA may treat a request to delete as a demand to cease communication under § 1692c(c), if the request is made in writing.

RMAI believes that flexibility is needed in determining the best means to allow consumers to make the requests in a manner that does not lead to confusing consumers of their rights under other law. Therefore, RMAI requests that the final rule reflects that a business subject to the FDCPA may choose “one or more methods” which are reflective of their usual interaction with consumers. Therefore, RMAI proposes the addition of § 7020(f):

¹⁶ *Spoofed FBI Internet Domains Pose Cyber and Disinformation Risks*, Federal Bureau of Investigation, Alert No. I-112320-PSA (Nov. 23, 2020) publicly available at <https://www.ic3.gov/Media/Y2020/PSA201123> and archived at <https://perma.cc/7GBQ-LLAY>.

¹⁷ *Id.*

¹⁸ See, 15 U.S.C. § 1692g.

¹⁹ See, *Mahon v. Credit Bureau, Inc.*, 171 F.3d 1197, 1202 (9th Cir. 1999) (“If no written demand is made, ‘the collector may assume the debt to be valid,’” citing *Avila v. Rubin*, 84 F.3d 222, 226 (7th Cir. 1996); 15 U.S.C. § 1692g(a)(3)).

A business that is a “debt collector” as defined by 15 U.S.C. § 1692a(6) shall only be required to provide an email address, mailing address or other means of electronic communication reflective of their usual interaction with consumers, for submitting requests to delete, requests to correct, and requests to know.

In this way, businesses subject to the FDCPA may define the channels of consumer communication that avoid consumer confusion and promote compliance with both the CCPA and other law.

§ 7022 Requests to Delete.

§ 7022(c)(4). The triggering event of proposed § 7022(c)(4) is not connected to the consumer requesting deletion. Section 7022(c)(4) proposes that certain service providers must be notified to delete the consumer’s personal information if “they may have accessed personal information from or through the service provider or contractor . . .” RMAI believes that what was intended as the trigger event is that the covered service provider *has* accessed the *requesting consumer’s* personal information. As proposed, such a notice must be provided even if the service provider never accessed the requesting consumer’s information, but *may* have accessed the personal information of other consumers. Therefore, RMAI, proposes the following:

Notifying any other service providers, contractors, or third parties that **may** have accessed the consumer’s 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. . .

§ 7023 Requests to Correct.

§§ 7023(f)(1); (f)(3). Proposed § 7023(f)(3) conflicts with the exemptions provided under § 1798.145(d)(1) and (d)(2) when consumer information implicates the federal Fair Credit Reporting Act (“FCRA”), 15 U.S.C. §§ 1681, *et seq.*

The exemption provided by the statute reads:

This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code . . .

Proposed § 7023(f)(3) also conflicts with the exemptions provided under § 1798.145(e) which provides that “[t]his title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102) . . .”

RMAI members regularly collect, process, sell or disclose personal information subject to both the Gramm-Leach-Bliley Act (“GLBA”) and the FCRA, and therefore the Act “shall not apply” to their activities with respect to this personal information.

However, proposed § 7023(f)(1) requires covered businesses when denying a consumer request to correct based on an “exception to the CCPA,” to explain to the consumer that such exception is a “basis for the denial.” Ostensibly, the phrase “exception to the CCPA” also means “exemption to the CCPA.”²⁰ Yet, proposed § 7023(f)(3) requires a covered business that denies a request to correct (even if the basis for denial is an exemption) to “[i]nform the consumer that, upon the consumer’s request, it will note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer.”

But when the basis for denial is an exemption to the CCPA, the Act “does not apply” and neither can the regulations promulgated pursuant to its authority.

Even if the Agency had authority to regulate personal information subject to the FCRA, § 7023(f)(3) would cause substantial disruption and conflict with the dispute handling regulations of 12 C.F.R. § 1022.43 (also known as the “Furnisher Rule”). The purpose of the Furnisher Rule is to ensure that furnishers of information to credit reporting agencies “implement reasonable written policies and procedures regarding the accuracy and integrity of information relating to consumers that they furnish . . .”²¹

One example of this irreconcilable conflict is that the Furnisher Rule recognizes certain disputes are frivolous, imposes standards for determining whether a dispute is frivolous and provides that “a furnisher is not required to investigate a direct dispute if the furnisher has reasonably determined that the dispute is frivolous or irrelevant.” 12 C.F.R. § 1022.43(f). No such standards exist for a request to correct. In fact, proposed § 7023(f) would permit a covered business to deny a frivolous request to correct, but then § 7023(f)(3) would require it to “inform any person with whom it discloses, shares, or sells the personal information,” such as a credit reporting agency, “that the accuracy of the personal information is contested by the consumer.” In the case of the frivolous dispute under the Furnisher Rule, 12 C.F.R. § 1022.43(f) would cause the covered entity *not to inform* credit reporting agencies of the frivolous dispute. Regardless, the

²⁰ We note that § 1798.185(3) allows the Agency to “establish[] any exceptions necessary to comply with state or federal law.” If that is the “exception” in proposed § 7023(f)(1) then it should be rephrased to state “exception to these rules.” In such instance we would understand that the proposed requirements of subsection (f) or wholly inapplicable if they implicate the *exemptions* contained in § 1798.145. However, because the § 7023(f)(1) refers to the “CCPA” and not these regulations, we do not believe it intended to only encompass exceptions under the regulations.

²¹ *The FCRA’s Requirement that Furnishers Establish and Implement Reasonable Written Policies and Procedures Regarding the Accuracy and Integrity of Information Furnished to all Consumer Reporting Agencies*, CFPB Compliance Bulletin 2016-01 (Feb. 3, 2016), p. 1, publicly available at https://files.consumerfinance.gov/f/201602_cfpb_supervisory-bulletin-furnisher-accuracy-obligations.pdf and archived at <https://perma.cc/9WEJ-9DVK> .

disruption should never occur because the Act “does not apply” to such personal information under both §§ 1798.145(d) and (e).

RMAI proposes the following revision to proposed § 7023(f)(1):

Explain the basis for the denial, including any conflict with federal or state law, ~~exception~~ exemption to the CCPA, exception to these regulations, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.

RMAI also proposes the following revision to proposed § 7023(f)(3):

Unless the basis for the denial is an exemption to the CCPA or an exception under these regulations, ~~Inform~~ inform the consumer that, upon the consumer’s request, it will note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer. The business does not have to provide this option for requests that are fraudulent or abusive.

§ 7026. Requests to Opt-Out of Sale/Sharing.

§ 7026(f)(2). Businesses cannot be required to notify third parties of opt-out requests when the sale or sharing of information is authorized by state or federal law, exempted by the CCPA, or excepted by these regulations.

As discussed in the comments to § 7023 above, the CCPA provides exemptions under §§ 1798.145(d)(1), (d)(2) and § 1798.145(e) when consumer information implicates the federal FCRA or GLBA. In both cases, the exemptions state “this title shall not apply” to the exempt information.

RMAI members will receive requests to opt-out of the sale or sharing of information. But RMAI members will likely possess only exempt information and, therefore, a consumer cannot opt-out of the sale or sharing of the exempt information. Nonetheless, proposed § 7026(f)(2) provides that *before* an RMAI member responds to a consumer in the allotted 15-business day period, it must “[n]otify[] 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 . . .” Thus, even though the Act “shall not apply” to the information in possession of RMAI members, proposed § 7026(f)(2) would require, arguably, immediate notification to covered “third parties” that a consumer has made an opt-out, even though it will be later denied. We understand that one purpose of the 15-business day period is to permit covered businesses sufficient time to determine whether it possesses covered consumer information. Proposed § 7026(f)(2) is inconsistent with this purpose and conflicts with the exemptions provided under §§ 1798.145(d)(1), (2) and 1798.145(e). RMAI proposes the following revision to § 7026(f)(2):

Notifying all third parties to whom the business has sold or shared the consumer's personal information which is not otherwise exempt from the CCPA or an excepted under these regulations, 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(k)(Proposed). Businesses should be permitted to deny requests to opt out of the sale or sharing of information when the sale or sharing is authorized by state or federal law, exempted by the CCPA, or excepted by these regulations.

A consumer cannot opt-out of the sale of personal information collected, processed, sold, or disclosed pursuant to the federal FCRA or GLBA, as explained above. The proposed revisions to § 7026, and particularly subpart (g), do not provide a business with the option to advise consumers of this exemption in response to a request to opt-out. In the case of requests to know, existing § 7024(e) allows a business to provide a response indicating that the information will not be provided "because of a conflict with federal or state law, or an exception to the CCPA." Likewise, proposed § 7023(f)(1), in the case of a request to correct, and § 7022(f)(1), in response to a request to delete, provide the business with the ability to respond with a denial analogous to that of existing § 7024(e). RMAI requests clarification that a business may similarly deny an opt-out request when the request conflicts with federal or state law or an exception to the CCPA. We believe that consumers will make combined requests to know, correct, delete and opt-out in a single communication. A business' response to the consumer should be consistent to avoid the risk of consumer confusion. RMAI proposes the following addition of § 7026(k):

In cases where a business denies a consumer's request to opt-out of the sale or sharing in whole or in part because of a conflict with federal or state law, exemption to the CCPA, or exception to these regulations, the business shall provide to the consumer an explanation identifying the applicable conflict with federal or state law, exemption to the CCPA or exception to these regulations.

§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.

§ 7027(m) (Proposed). Businesses should not be required to notify third consumers of their right to limit the use and disclosure of sensitive personal information when the use and disclosure is authorized by state or federal law, exempted by the CCPA, or excepted by these regulations.

As discussed above, the CCPA provides exemptions under §§ 1798.145(d)(1), (2) and § 1798.145(e) when consumer information implicates the federal FCRA or GLBA. In both cases, the exemptions state "this title shall not apply" to that information. Many RMAI members only possess exempt information and, therefore, a consumer cannot effectively request limitations. However, proposed § 7027 does not contemplate the effect of the exemptions. Instead, proposed § 7027(b) requires such businesses to provide "two or more designated methods for submitting

requests to limit.” Proposed § 7027(f) allows a business to deny a fraudulent request to limit, but provides no guidance on denying a request to limit. Finally, proposed § 7027(l) creates seven exceptions for purposes for which a business may disclose or use such information and not “offer consumers a right to limit . . .” It necessarily follows that businesses that use or disclose sensitive information that is exempt from the CCPA should also not “offer consumers a right to limit . . .”

Therefore, RMAI proposes the addition of § 7027(m):

A business that only uses or discloses sensitive personal information exempt from the CCPA is not required to post a notice of right to limit.

§ 7028. Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information.

§ 7028(c). Proposed subpart (c) can be reasonably interpreted to mean that a consumer gains certain rights simply because they have “exercised their right to limit.” However, as discussed above, the CCPA provides exemptions under §§ 1798.145(d)(1), (2) and § 1798.145(e) when consumer information implicates the federal FCRA or GLBA. In both cases, the exemptions state “this title shall not apply” to the exempt information. Therefore, a consumer who makes a request to limit exempted information has gained no rights with respect to the exempt information. Further, proposed subpart (c) excludes sensitive personal information subject to “subsection (l)” which we understand means § 7027(l). That subsection creates seven categories of purposes for which a business may disclose or use such information and not offer a right to limit.

Because proposed § 7028(c) provides treatment for the exceptions created by § 7027(l), RMAI believes it must also give treatment to information exempted by the CCPA. After all, it is possible for a consumer to have exercised a right to limit applicable to non-exempt information, while remaining ineffective against exempt sensitive personal information. We foresee situations in which business who market products but also provide financial services may possess both.

RMAI proposes revisions to § 7028(c) as follows:

If a consumer who has exercised their right to limit initiates a transaction or attempts to use a product or service that requires the use or disclosure of sensitive personal information for purposes other than those set forth in subsection (l) or exempted by the CCPA, the business may inform the consumer that the transaction, product, or service requires the use or disclosure of sensitive personal information for additional purposes and provide instructions on how the consumer may provide consent to use or disclose their sensitive personal information for those additional purposes. The business shall comply with section 7004 when obtaining the consumer’s consent.

Article 4. Service Providers, Contractors, and Third Parties

§ 7051. Contract Requirements for Service Providers and Contractors.

§ 7051(a)(7). RMAI suggests that the phrase “in a manner consistent with the business’s obligations under the CCPA and these regulations” could be more precise and helpful by citing to, or describing with more detail, those obligations.

Article 9. Investigation and Enforcement.

§ 7302. Probable Cause Proceedings.

§ 7302(d). Civil Code § 1798.199.55, states that probable cause hearings will be “conducted in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500), Part 1, Division 3, Title 2, Government Code). However, it is not clear from that Act what timeframe would apply to the issuance of an agency’s probable cause determination. RMAI recommends that this subsection specify the timeframe in which the written decision will be issued.

§ 7304. Agency Audits.

§ 7304(c). RMAI respectfully disagrees with the concept of unannounced audits. Audits typically require the dedication of significant resources on the part of a business and, without prior announcement, could seriously disrupt the ability of a business to provide goods or services to consumers. RMAI suggests that if this option is to be exercised at all, it be limited to businesses that have violated the CCPA and are subject to continuing supervision.

III. CONCLUSION

RMAI thanks the California Privacy Protection Agency for its many thoughtful modifications to the proposed rules and for its consideration of these comments.

If you have questions or if we can be of any assistance, please contact RMAI General Counsel David Reid at [REDACTED] or (916) 482-2462.

Sincerely,

[REDACTED]

Jan Stieger
RMAI Executive Director

From: **Matt K.** [REDACTED]
To: **info@CPPA** <info@cpha.ca.gov>
CC: [REDACTED]
Subject: an idea to solve privacy problems
Date: 25.08.2022 09:27:38 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

I'm writing to suggest a simple idea...

Why not pass a law that requires the "default" setting for everyone's personal data to be "opted out" of data sharing? Furthermore, a person couldn't be denied, on that basis, the right to participate in essential online services, however they would need to take deliberate action (ie- "opt-in") to permit sharing of their personal data.

If you could enforce such a law, that would solve the problem for 99% of people.

Matt Kurlan

Carlsbad, CA

From: **joseph** [REDACTED]
 To: **Regulations** <Regulations@coppa.ca.gov>
 Subject: Cookies
 Date: 25.08.2022 10:23:44 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Get pocket.com makes it clear with a large reject all button.

Medicine.net is an example of deceptive practices regarding cookies or the "Privacy manager."

It opens up with a blue bar that says "I accept" and a transparent bar that says "Manage settings", which tells you which cookies are always active and has 13 switches for the others but it does not say if the switch in the on position allows cookies or rejects them. If you turn the switch to the right it turns blue. Does that mean you Accept the cookies as in the previous page or reject the cookies.

Medicine.net does not make the choices clear.

Medicine.net has 4 always active, 13 with switches, and 4 more always active at the bottom. The language that they use to identify the cookies are, "Legitimate Interests" not cookies.

The switch is in an off position it is not in an accept or reject position. By activating the switch Am I accepting the "legitimate interests" or am I rejecting the "legitimate interests?"

It doesn't call them cookies.. It's unlikely that they are all automatically rejected if you do nothing when 13 switches are in the dark mode.

When I go to a website to get legitimate medical information I don't expect to be deceived right off the bat.

When the choice is unclear I just close the page knowing I can't trust what I'm about to read. Medicine .Net is one of those sites.

From: **Robin West** [REDACTED]
 To: **info@CPPA** <info@cpga.ca.gov>
 Subject: Re: I wish to speak- is it Aug 24 or 25
 Date: 25.08.2022 10:32:36 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

I was acknowledged and spoke up.

But I pressed *9 several times before the conference ended and I was NOT acknowledged. I had to dial the 216 tel number and enter my passcode a couple times, just to be able to hear.

Oh well I am disappointed because when I made my CCPA request in written form, Nordstrom US mailed me 55 pages of computer gibberish which is completely illegible. I think they are trying to cover up the fact they breached my security and used a false DOB for me to report to the credit bureaus. They created two VISA accounts for me by doing this, and it caused me problems. In addition there is evidence they allowed someone with my same name to interfere with my ability to purchase. Now they have gone so far to retaliate against me and they set me up, involving an African American Walnut Creek police officer, along with several other African American employees. Now I cannot ever shop at Nordstrom again. I have had a Nordstrom card since 1986, and always had a good relationship, until I made my CCPA request.

I was hoping to get some suggestions as to how to handle the retaliation issues which arose after I made my CCPA request of Nordstrom.

Is there a way to speak to the committee regarding this severe retaliation against me, by Nordstrom ?

Thank You

Robin L West

NOW NORDSTROM REFUSED TO COMPLY WITH MY CCPA REQUEST

On Thu, Aug 25, 2022 at 9:23 AM info@CPPA <info@cpga.ca.gov> wrote:
 Ms. West.

I see you on now. We will call you next.
 When called upon, please press star-6 to unmute.

From: Robin West [REDACTED]
 Sent: Thursday, August 25, 2022 4:20 PM
 To: info@CPPA <info@cpga.ca.gov>
 Subject: Re: I wish to speak- is it Aug 24 or 25

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

NOTHING HAPPENS WHEN I PRESS 9

On Thu, Aug 25, 2022 at 9:19 AM info@CPPA <info@cpga.ca.gov> wrote:
 Please press *9 to raise your hand to speak. You will be called on, then can press *6 to mute/unmute.

From: Robin West [REDACTED]
 Sent: Thursday, August 25, 2022 4:18 PM
 To: info@CPPA <info@cpga.ca.gov>
 Subject: Fwd: I wish to speak- is it Aug 24 or 25

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

I joined the call and I am Robin West.

I do not know how to speak. I am listening to Ben with the Chamber.

Will I be called and unmuted to speak ????

----- Forwarded message -----

From: **info@CPPA** <info@coppa.ca.gov>
Date: Thu, Aug 25, 2022 at 9:07 AM
Subject: Re: I wish to speak- is it Aug 24 or 25
To: Robin West [REDACTED]

Ms. West

You may join the meeting by dialing the number below and using the conference code: 682962

By Telephone: USA (216) 706-7005 US Toll
USA (866) 434-5269 US Toll-free
Conference code: 682962

From: Robin West [REDACTED]
Sent: Thursday, August 25, 2022 4:03 PM
To: info@CPPA <info@coppa.ca.gov>
Subject: Re: I wish to speak- is it Aug 24 or 25

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

WHERE IS MY ACCESS CODE ????????

I JUST CALLED 216-706-7005 AND I WAS ASKED FOR AN ACCESS CODE. YOU

DID NOT GIVE ME ONE !!!!!!!!!!!!!

PLEASE PROVIDE ME WITH AN ACCESS CODE SO I CAN JOIN AND SPEAK AT THE PUBLIC HEARING WHICH IS STARTING NOW.

Robin L West (Walnut Creek) [REDACTED]

On Mon, Aug 22, 2022 at 8:32 AM info@CPPA <info@coppa.ca.gov> wrote:

Ms. West

Thank you for your inquiry.

You may RSVP to speak at the upcoming Rulemaking hearings here:
<https://cppa.ca.gov/webapplications/rsvp>

From: Robin West [REDACTED]
Date: Saturday, August 20, 2022 at 7:39 PM
To: info@CPPA <info@cppa.ca.gov>
Subject: I wish to speak- is it Aug 24 or 25

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello

I wish to speak up about my experience with privacy breaches, fraud in ALL of my records and accounts, and about business failing to respond or fulfill my explicit CCPA requests, and about the importance of the oversight committee/ regulatory or whatever your new group is called. I hope there will be penalties for the companies who are in non compliance.

Regards

Robin L West

Sent from my iPhone

From: **D. Shackelford** [REDACTED]
 To: **Regulations** <Regulations@cpha.ca.gov>; **info@CPA** <info@cpha.ca.gov>
 CC: **D. Shackelford** [REDACTED]
 Subject: Re: They Said Ask You. Fw: Automatic reply: How to get into comment queue?
 Date: 25.08.2022 20:31:49 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello again,

I did attend by land line phone again this morning. I was unable to get the *9 and *6 to work for making my comments, so I have included them here.

1. Our State has survivors of abusive predators. These folks are trying to live Safe at Home but are at risk of severe harm with their information currently assumed to be owned & shareable by web based company and government forms-access/virtual-meeting/or contact-us sites. Do not track, Do not share and other existing modalities of self protection are not being honored by the web of today. Some sites even presume to claim the ability to use people's zoom or Facetime image in their advertising without notice or compensation! Most government sites are dependent on the automated web based systems making my participation blockage of today far from a rare occurrence, so these hazardous policies are not avoidable by just not joining social media sites anymore.

I hope the CPA can include some special penalties for violations against these folks. Their lives may depend upon it.

2. Web sites routinely time out user participation before the Privacy Policy/TOU embedded links can be reviewed. This makes it nearly impossible for users to self administer informed consent to the invasions exposed in these currently "industry standard" documents. I hope this can be updated to user friendly vs user abusive.

3. I feel that any maximum time frame that it takes for an Opt-Out request to be processed by a business entity needs to be reflected as a minimum +1 day allowable time-frame for the sharing (of any kind) or aggregating of data from user participation. This is the only way that the spirit of an Opt-out can be upheld. I see companies disavowing responsibility for what third party sites do with data they have shared today while insisting the public be patient with a 40+ days (of automated replication of information to affiliated systems) response to these Opt-Out request adherence. If they can't pull it back they should not be absolved for sending it out; in my opinion.

4. For this last item I will introduce myself as a mobility challenged veteran who has leveraged internet access for remote medical participation and family connections for over a decade. I have experience receiving push ads that indicate my video medical appointment had been data leaked by the equipment. It is the equivalent of getting ads for left hand baseball gloves minutes after speaking to my doctor about a broken right wrist! For my medical privacy this is a metaphor example not a specific detail one.

If this continues to be allowed no one has privacy to avoid discrimination on the basis of what should be private health status. I think this must be a HIPPA violation some how? In the data tracked and retained digital age this will impact the employ-ability and housing availability of ourselves as elders, our children as American dream house buyers, and our grandchildren as suitable for employment. The thing about discrimination is that when it can be done anonymously thru secretly aggregated data there is no way to hold the malicious actors accountable.

Thanks for retaining enough redundancy for me to submit these comments. I wish some of the corporate decision makers could have heard my experienced user side of the story thru the technology today. My home internet is data crippled at the moment so I am re-experiencing the demanded rights wavers to use public access. No, I did not spend my 1hr of access reading the privacy policy for this public web access site. I have read previous versions and hope my Creator will provide whatever protection my need to be heard has overlooked the need for yesterday & today. 20+ years of caution possibly blown in two hours of home digital outage. Frustrating, but true.

Best Regards to whomever this should go to and thanks for patience of the other parties,

D. Shackelford

P.S. you are welcome for the backwards compatibility beta testing. I could not be heard, but did here staff trying to fix connectivity sound issues as well as much of the meeting itself. d.s.

On Wednesday, August 24, 2022, 3:50:53 PM PDT, D. Shackelford [REDACTED] wrote:

FYI Public possibly being looped by the automated systems...

----- Forwarded Message -----

From: info@CPPA <info@coppa.ca.gov>

To: D. Shackelford [REDACTED]

Sent: Wednesday, August 24, 2022, 3:39:26 PM PDT

Subject: Automatic reply: How to get into comment queue?

Thank you for your email. Please note that this is a general mailbox for the California Privacy Protection Agency.

PRESS:

For press inquiries, please email press@coppa.ca.gov

MEETINGS & EVENTS:

Information about upcoming meetings and events are available on our website at <https://coppa.ca.gov/meetings/>.

Recordings, transcripts, and materials from our Meetings & Events will be made available on our website and Youtube channel shortly after they've been processed.

REGULATIONS:

For questions about our upcoming rulemaking, please visit <https://coppa.ca.gov/regulations/> to see our current rulemaking activities and signup for our mailing list. If you would like to submit a public comment on an ongoing rulemaking, please email the written comment to regulations@coppa.ca.gov.

CONSUMER COMPLAINTS:

For questions about enforcement, including consumer complaints, please note that administrative enforcement of the California Consumer Privacy Act by the California Privacy Protection Agency does not commence until July 1, 2023. The

California Attorney General's Office is currently responsible for all California Consumer Privacy Act

enforcement. Accordingly, complaints and enforcement-related questions should be directed to the California Attorney General's Office. You can contact them via the Attorney General's Complaint Form: <https://oag.ca.gov/contact/consumer-complaint-against-business-or-company> or the Attorney General's Office of Consumer Privacy Tool: <https://oag.ca.gov/consumer-privacy-tool>.

PUBLIC RECORDS ACT REQUESTS:

For questions regarding PRA requests, please email: legal@cpga.ca.gov with the Subject: ATTN: PRA Coordinator

Or via paper mail to: CPPA ATTN: PRA Coordinator 2101 Arena Blvd Sacramento, CA 95834

Fees are determined by the number of copies and availability of the documents/records requested. CPPA will tell you the final cost. You must pay the fees before CPPA can release the documents/records.

Thank you for emailing the CPPA.

To the CPPA:

I offer my views on the proposed CPRA regulations.

Section 7001 - Definitions

The term “precise geolocation” is not defined, which incentivizes less scrupulous businesses to interpret this term loosely to make more money. Without a clear definition, it will be difficult to bring enforcement actions against such businesses.

I recommend that the CPPA adopt the same definition as the Network Advertising Initiative, which requires the truncation of latitude and longitude to two decimal places, corresponding to resolving the actual location of a user or device to within the area of a circle with a radius of at least 500m.¹ This essentially means that users will be targeted to an area the size of Central Park in Manhattan.

“Precise geolocation” means identifying a consumer with more precision than longitude and latitude with two decimal places, or within the area of a circle with a radius of less than 500 meters with an accuracy of 68% or more.

This definition also tracks functionality for reducing precision within the Android and iPhone development tools, according to the NAI document I cited above.

With such a clear definition, it will be easy for consumers to tell when technology companies are abusing precise geolocation information. Many ad campaigns are “geo fenced” – sending ads to consumers who visit specific places. A consumer who gets a campaign which is obviously geofenced will have reason to investigate and make a complaint against the business.

Section 7001 - Definitions

The definition of “unstructured” is not correct. It says that information in a text file is unstructured, however an XML file is a text file and is structured. (Some databases such as Apple’s CoreData can work natively with XML databases.) The Wikipedia’s definition is better.

“Unstructured” as it relates to personal information means personal information that either does not have a pre-defined data model or is not organized in a pre-defined manner.

Section 7012 - Notice at Collection of Personal Information

Section 7012(e)(6) states *“If a business allows third parties to control the collection of personal information, the names of all the third parties; or, in the alternative, information about the third parties’ business practices.”* However, the regulations do not make clear that a business

¹ See “Guidance for NAI Members: Determining Whether Location is Imprecise,” Network Advertising Initiative, Feb 2020

controlling the collection of personal information would be a third party. For example, consider a technology company which has a pixel on a business's website. The technology company could take the position that it is collecting personal information directly from consumers and therefore is not a third party. To avoid ambiguity, I recommend this change:

If a business allows one or more other businesses to control the collection of personal information, the names of all such businesses (which shall be deemed to be third parties); or, in the alternative, information about such businesses' (which shall be deemed to be third parties) business practices."

Section 7025 - Opt-Out Preference Signals

Section 7025 has the fundamental issue that it does not meet the requirements of Section 185(a)(19) of the CPRA which requires the CPPA to be specific about the opt-out preference signal which businesses are required to recognize. The draft regulations allow "*any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing.*" The obvious intent is to require that the Global Privacy Control (as specified on globalprivacycontrol.org) be recognized. However, by being vague and non-committal, less scrupulous websites will say that they are being compliant by recognizing a signal not commonly implemented, and will offer spurious reasons why they choose not to recognize the GPC. To solve the issue, I recommend this change: ~~to 7025(b)~~

A business shall process the opt-out preference signal that conforms to the specifications published on globalprivacycontrol.org, provided that the signal is sent by a 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.

I retain the language about the intent of the use of the signal because it will inevitably be the case that some web browsers set the GPC flag by default, as this happened with "do not track" many years ago. These web browsers can be detected (whether by the "User-Agent" HTTP header or some other means) and their GPC signals can be blocked as invalid, at the option of the website.

I note that the language 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*" is contradictory to the sentence that "*The configuration or disclosure does not need to be tailored only to California or to refer to California.*" because no other jurisdiction has such a peculiar definition of "sale" or "sharing" as California does, but I don't have a strong enough opinion to offer a suggestion.

With respect to subsection (e), in my opinion it is not a defensible statement of the law. The CPRA clearly gives businesses a choice between posting opt-out links and honoring an opt-out

preference signal. The CPPA has interpreted the law to mean that the latter is a “frictionless” preference signal, and required that all businesses honor the preference signal whether frictionless or not. I believe that this too-cute-by-half rulemaking puts the CPRA regulations at risk of being overturned in litigation, and in my view subsection (e) should be deleted. Note that as a practical matter, as other states (e.g., Connecticut) have already required that the GPC be honored so nothing would be lost by taking out this section.

With respect to subsection (f)(2), this shows a misunderstanding of what an opt-out of “sale” means. While the CPRA was motivated by animus towards technology companies², the CPRA in fact applies to many other situations not related to advertising where personal information is disclosed by a business to another. For example, it may transmit personal information as part of the consumer’s intended service. Subsection (f)(2) requires that “[a] consumer who uses an opt-out preference signal shall have the same experience with regard to how the business’s product or service functions compared to a consumer who does not use an opt-out preference signal.” Imagine a bank performing bill-pay services for a consumer. Obviously, paying bills on behalf of a consumer means disclosing personal information about the consumer to a third party. Now imagine that the consumer activates the GPC and visits the website of the bank, which chooses to “frictionlessly” honor the GPC. That means that the bill-pay service will be stopped with no immediate notification to the consumer. Clearly, no bank will choose to “frictionlessly” honor the GPC for precisely this reason, but the point should be clear that in many cases, the use of an opt-out signal will imply that the consumer’s experience will be different. I recommend the deletion of subsection (f)(2).

Section 7027 - Requests to Limit Use and Disclosure of Sensitive Personal Information

This section should clearly state whether the use of precise geolocation information is allowed for the purpose of advertising. The primary reason that so many apps track users’ location is for ad monetization. For example, today Starbucks can send ads with coupons to consumers who are inside a Starbucks. Or IKEA could show ads to consumers who have been near an IKEA in the last 30 days. Failing to be specific about the use of precise geolocation information by advertisers will allow the sleaziest technology companies to continue doing what they are doing.

In subsection (l)(1), I recommend one of these two edits, depending on the CPPA’s view:

To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. For example, a consumer’s precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to specific location. A consumer’s precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information. Additionally, the use of precise geolocation information for the purpose of selecting and delivering

² See “The Unlikely Activists Who Took On Silicon Valley — and Won,” NY Times, Aug 14, 2018

advertisements is presumed to be not reasonably expected and is therefore prohibited under the CPPA.

or

To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information. The use of precise geolocation information solely for the purpose of selecting and delivering advertisements (without storing such information or building profiles) is presumed to be reasonably expected in an ad-supported content application.

Section 7050 - Service Providers and Contractors

With respect to subsection (c), please clarify whether the service provider exception is available to media companies running advertisements. As you likely know, the advertising industry created the Limited Service Provider Agreement in 2019 whereby the entire advertising industry would operate as service providers of individual websites.³ The intent was that personal information would flow almost as freely as if the information were "sold," but without accountability. It is true that "advertising and marketing services" are allowable business purposes, but it is ambiguous as to whether these are limited to advertising for an advertiser. If the CPPA disagrees that this is a permissible use of the service provider exception, language such as the following could be used:

A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but those services shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or from its own interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor. Moreover, such a business must be the advertiser, not the media company, in the transaction. Illustrative examples follow.

Section 7051 - Contract Requirements for Service Providers and Contractors

³ Available at <https://www.iabprivacy.com/lspa-2019-12.pdf>

The CPRA itself gave businesses two years to update their contracts to meet certain new requirements. However, the draft regulation has provided its own list of what is required in CPRA-compliant contracts. Because this list is subject to change between now and when the regulations are finalized, nobody knows what requirements will be in the final regulations. I'm guessing that companies who had invested vast resources into becoming compliant have now halted these efforts pending final regulations.

As the statement of reasons says, it is true that the various contract requirements are set out in the statute, however the statutory requirements do not all apply to both the business and service provider. The requirements in Section 100 apply to the business, the ones in Section 140 apply to the service provider. If (due to bad legal advice, or any other reason) parties have entered into a contract meeting only the Section 140 requirements, the service provider should not lose its protections under the statute. I would urge the CCPA to change the regulation: in 7051(a):

For both the business and the service provider or contractor to meet their requirements under the CCPA, the contract required by the CCPA shall:

Subsection (c) may give bad-faith actors reason to argue that they are not third-parties. As you know, the original CCPA led to spurious theories that one could be neither a service provider nor a business, or that a lack of "consideration" was a widely available loophole to advertising companies and other companies whose business relied on the exchange of personal information. I recommend changing the word "may" to "generally would" to affirm that no-sale situations are the exception not the rule.

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 generally would be considered a sale for which the business must provide the consumer with the right to opt-out of sale/sharing.

Subsection (e) is vague and imposes an unreasonable amount of uncertainty. It implies that a certain amount of auditing is required to maintain the service provider exception, however in reality businesses do not conduct privacy audits of their counterparties even in Europe. I urge that this section be deleted, because if a business has reason to believe that its "service provider" is violating the rules, and that is enough to defeat the service provider exception, then nothing more needs to be said.

Many service provider contracts have been entered into in reliance on the original CCPA statute, and asking businesses to repaper these contracts simply to include boilerplate is a tremendous waste of resources. I ask for a "grandfather clause."

p. 5

(f) A contract between a business and service provider meeting the statutory and regulatory requirements in effect on December 31, 2022 shall be deemed to meet the requirements until such time that the contract is amended for any reason.

Section 7053 - Contract Requirements for Third Parties

This section requires that a business “selling” information to a third party put in place a contract with certain boilerplate provisions.

Subsection (c) states that if a third party is not subject to such a contract, that it is bound by the requirements anyway. This is plainly inconsistent with the CPRA which put the obligations entirely on the disclosing party. Subsection (c) should be deleted.

Subsection (d) states that “A third party shall comply with the terms of the contract required by the CCPA and these regulations.” This is also inconsistent with the CPRA, for the same reasons, or redundant with the CPRA. Subsection (d) should be deleted.

Subsection (e) is vague and imposes an unreasonable amount of uncertainty. It implies that a certain amount of auditing is required even with a third-party which goes even further beyond what is reasonable for data protection regulations. (In Europe, only “processors” are audited, not “controllers.”). I urge that this section be deleted, because if a business has reason to believe that its third party recipient is violating the rules, and that is enough to ascribe liability to a business, then nothing more needs to be said.

Section 7062 - Verification for Non-Accountholders

My concern is that technology companies can use a bad-faith justification of fraud prevention to deny consumers the right to exercise their rights. An example should be provided for advertising technology companies who have personal information (but not personally identifiable information) about consumers:

Example 2: If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 7060, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device. Alternatively, a business may have collected information from web browsers or mobile devices to build a profile for targeting advertising and not have knowledge of consumers' real-world identities. The business should ask the consumer to confirm information from the profile.

p. 6

CPRA

for example the geographic region from which the web browser or mobile device is frequently used. It is a violation of the CPRA for a business to systematically fail to honor consumer requests on the basis that the device may be shared among household members or on the basis that a cookie ID or mobile device ID are insufficient to identify a consumer.

New Section - Business Purposes

Section 185(a)(10) of the CPRA asks the CPPA to define additional business purposes.

Issuing regulations further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers' personal information consistent with consumers' expectations, and further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140.

The existing definition does not specifically allow for cloud computing and cloud storage services, where computer capacity is rented for the sole use of the customer. For example, Amazon Web Services offers cloud computing in the form of its Elastic Cloud Compute service and cloud storage in the form of its Simple Storage Service, to name a few. Both EC2 and S3 keep customer data encrypted and strictly separated. Amazon has provided service provider terms to its customers,⁴ however these terms do not identify which "business purpose" Amazon is providing.

Anecdotally, it seems that people treat the list of business purposes as suggestive examples. If a service seems like the kind that a service provider ought to provide, people go ahead and sign service provider contracts, regardless of whether the service is actually listed as a business purpose in the statute. Unless action is taken to make the list of business purposes more complete, the result will be nearly universal disregard of the business purpose limitation. My suggestion is to include cloud computing and storage, as these are the most obvious business purposes currently missing from the list.

The list of allowable business purposes under section 140(e) shall include: cloud computing and cloud storage (provided that the business has sole control of the processing of the personal information).

⁴ "AWS CCPA Terms" available at https://d1.awsstatic.com/legal/aws-ccpa/AWS_CCPA_Terms.pdf