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 Reports[1] 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 CPPA 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 a 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-priva.html?edition=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 way[28] — 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 (justin.brookman@consumer.org) for more information.