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)

By

Justin Brookman, Director of Technology Policy
Maureen Mahoney, Senior Policy Analyst
Nandita Sampath, Policy Analyst

November 8, 2021

Table of Contents

I. Introduction

Consumer Reports[1] appreciates the opportunity to provide preliminary comments on the proposed rulemaking under 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), as amended by Proposition 24, work for consumers.

Privacy laws should protect consumer privacy by default, through strong data minimization that limits data use, collection, sharing, and retention to what is reasonably necessary to provide the service requested by the consumer.[3] But at the very least, opt outs should be workable for consumers. It's essential that the regulations clarify that businesses are required to honor browser privacy signals, including the Global Privacy Control specifically, as an opt out of sharing and sale.[4] Even with such a requirement in the current CCPA regulations,[5] and guidance from the AG that businesses must honor Global Privacy Control signals as an opt out of sale,[6] many companies have simply disregarded this right.[7] Second, when a consumer opts out, the CPPA must not permit companies to make their personal information available to third parties for a commercial purpose. Otherwise, key rights will not be accessible in practice for consumers.

The rulemaking also provides a prime opportunity to set baseline protections with respect to automated decision-making. Though automated decision-making can have discriminatory effects, it is largely unregulated. We urge the CPPA to adopt key protections with respect to transparency and auditing of the algorithms used in important decisions that affect consumers, and to prohibit uses that lead to egregious harms.

---

[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] *Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020*, CALIFORNIA PRIVACY PROTECTION AGENCY (Proceeding No. 01-21) (Sept 22, 2021), [hereinafter "Invitation for Comments"] https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

[3] *Model State Privacy Act*, CONSUMER REPORTS (February 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

[4] Global Privacy Control, https://globalprivacycontrol.org/ (last visited Nov. 6, 2021).

[5] Cal. Code Regs tit. 11 § 999.315(c).

[6] State of California Department of Justice, California Consumer Privacy Act, Frequently Asked Questions (FAQs), at B(7), (last visited Nov. 7, 2021), https://oag.ca.gov/privacy/ccpa.

[7] Russell Brandom, *Global Privacy Control Wants to Succeed Where Do Not Track Failed*, THE VERGE (Jan. 28, 2021), https://www.theverge.com/2021/1/28/22252935/global-privacy-control-personal-data-tracking-ccpa-cpra-gdpr-duckduckgo.

Below, we outline key recommendations to uphold consumer privacy and advance civil rights, consistent with the CPRA.

II. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information

Too many companies have failed to adhere to the letter and spirit of the California Consumer Privacy Act, and Consumer Reports has found that some consumers have run into difficulties when attempting to opt out of the sale of their information under the CCPA.[8] Without clarifying regulations specifying that companies adhere to browser privacy signals as a global opt out of sale, consumers will have few options but to opt out at every company one by one, even though there are hundreds, if not thousands, of companies that sell consumer data.[9] In addition, Consumer Reports has found that some companies have ignored the opt out with respect to behavioral advertising, and instead send consumers to ineffective third-party industry sites.[10] And finally, it can be particularly time-consuming to opt out at certain companies — some even require consumers to download separate, third party apps to stop the sale of their data.[11]

a. <u>The CPPA should clarify that compliance with global privacy controls is mandatory under the CPRA.</u>

The CPPA should issue clarifying regulations specifying that compliance with global privacy signals is not optional, but mandatory under the CPRA. Due to the complexity of the CPRA's language, there has been some ambiguity as to whether companies must always comply with such signals. Section 135 — which details how companies must respond to requests to opt out of the sale of data — provides two different possible paths to compliance in Section 135(a) and Section 135(b). Only Section 135(b) specifically mentions complying with global opt-out signals; as a result, several reporters[12] and law firms[13] have stated that companies may choose to ignore global opt-out signals if they opt to comply with Section 135(a) instead of Section 135(b).

---

[8] 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.

[9] See, for example, State of California Department of Justice, Data Broker Registry (last visited Nov. 7, 2021), https://oag.ca.gov/data-brokers (includes approximately 500 data brokers).

[10] Maureen Mahoney et al., *The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act*, CONSUMER REPORTS at 16 (Feb. 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf.

[11] *Are Consumers' Digital Rights Protected?, supra* note 8, at 24.

[12] Wendy Davis, *Ad Industry Protests California AG's Proposed Privacy Rules*, MEDIAPOST (June 9, 2020), https://www.mediapost.com/publications/article/352362/ad-industry-protests-california-ags-proposed-priv.html.

[13] Kate T. Spelman, David P. Saunders and Effiong K. Dampha, *New Draft of California Privacy Ballot Initiative Released*, JENNER & BLOCK (last visited Nov. 6, 2021), https://jenner.com/system/assets/publications/19414/original/2019%20Data%20Privacy%20and%20Cybersecurity%

Such a reading of the statute is inconsistent with the purpose of CPRA as well as the plain language of Section 135(e) which plainly states that companies must honor global privacy control opt-out requests *regardless* of whether a company complies with Section 135(a) or Section 135(b). Section 135(e) provides:

> A consumer may authorize another person to opt-out of the sale of sharing or 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) of this Section, 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 of 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) of this Section. For purposes of clarity, a business that elects to comply with subdivision (a) of this Section may respond to the consumer's opt-out consistent with Section 1798.125.

This language clearly states that a consumer may designate another person to exercise their privacy rights on their behalf — including through a global opt-out preference signal — and such a request must be honored regardless of whether the company has chosen to comply with Section 135(a) or Section 135(b).

Such a reading is also consistent with the bifurcated compliance structure of Section 135. Under Section 135(a), companies must include clear and conspicuous links on their internet homepage labeled "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information." However, if a consumer endeavors to exercise either of these rights, they may bargain with the consumer, asking for permission to disregard the opt-out request (whether a signal or an individual request) pursuant to rules laid out in Section 125 of the statute.

Section 135(b), on the other hand, allows a company to not place prominent "Do Not Sell" or "Limit the Use" links on their site so long as they do not bombard users with consent dialogs or enticements seeking to disregard an opt-out request. Instead, the company can only provide a link through which consumers can later change their preferences. This section was designed to encourage companies to not deluge consumers with permission requests as has been the experience with websites under the GDPR and the ePrivacy Directive in Europe.[14]

20_%20New%20Draft%20of%20California%20Privacy%20Ballot%20Initiative%20Released%20-%20ATTORNEY%20ADVERTISING.pdf.

[14] *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent,* PRIVACY INTERNATIONAL (May 21, 2019), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent.

To interpret Section 135(a) as letting companies ignore global preference signals would on the other hand strongly encourage companies to comply with Section 135(a) instead; the ability to disregard easily expressed global preferences would strongly outweigh any marginal benefits from not having to include opt-out links of a company's website. Such a reading would be inconsistent with the purpose of providing Section 135(b) at all. Fortunately, Section 135(e) is explicit that under both paths, companies must honor global preference signals.

Moreover, companies are already required to honor global privacy controls under the CCPA today.[15] There is no rationale for interpreting CPRA — which has the stated intent of strengthening the CCPA[16]— as weakening one of CCPA's core protections. Indeed, without global privacy controls and comparable scalable options, California's opt-out rights are not meaningfully usable by consumers. A Consumer Reports study of CCPA opt-out rights in October 2020 found that it could be very difficult for consumers to stop the sale of their information. About 14% of the time, broken or inaccessible opt-out processes prevented consumers from opting out of the sale of their information.[17]

Consumers deserve an easy and practically usable way of globally expressing certain privacy preferences. The CPPA should put an end to any uncertainty around the CPRA's language and issue clarifying language that covered companies must always honor global preference signals that comply with the statute's requirements.

b. <u>The CPPA should provide and regularly update a list of global privacy signals that must be interpreted by companies as an opt-out signal.</u>

Currently, there is no definitive list of what "user-enabled global privacy controls" companies must treat as legally valid opt-out requests under the CCPA.[18] In January 2021, then Attorney General Becerra tweeted that CCPA mandates that companies honor the Global Privacy Control, at the very least.[19] Since then, the Attorney General's office has updated the CCPA FAQs to formalize that GPC opt outs are legally binding,[20] and the office has stated that it has

[15] Cal Code Regs tit. 11 § 999.315(c).
[16] California Privacy Rights Act of 2020 §§ 3, 3(C)(1); see also *Crafting Better Privacy Laws, Based on the California Model: A Conversation with Alastair Mactaggart*, WIREWHEEL (Jul. 20, 2021), https://wirewheel.io/ccpa-state-privacy-laws/ (Mactaggart is quoted, "One of the great benefits of California's law is that it allows for my device, my global setting, my phone, my computer to do it for me.")
[17] *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?, supra* note 8.
[18] Cal. Code Regs. tit. 11 § 999.315.
[19] @AGBecerra, Twitter (Jan. 28, 2021), https://twitter.com/AGBecerra/status/1354850321692934144.
[20] State of California Department of Justice, California Consumer Privacy Act, Frequently Asked Questions (FAQs), *supra* note 6, at B(7).

begun sending warning letters to companies who do not comply with the signal.[21] However, there is no clear guidance on the legal status of any other global controls or browser settings.

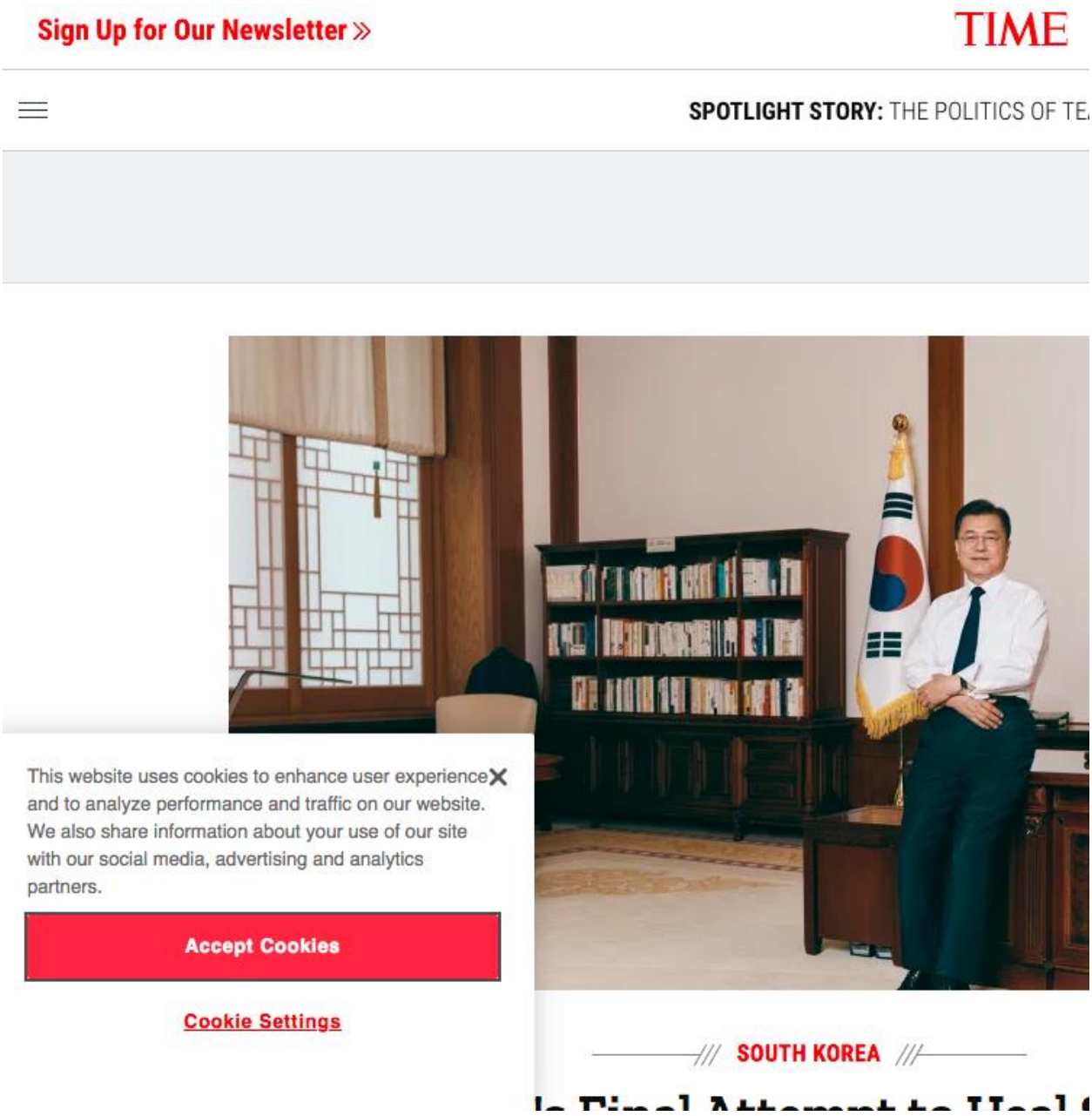
The CPPA should create and regularly update a list of signals and settings that should be treated as legally binding requests under the CPRA. The Global Privacy Control, with over 50 million unique users each month, should be designated as conveying a legally binding request to opt out of the sharing or selling of a user's personal information under Section 13. The CPPA should consider giving similar status to other comparable settings, including the "Do Not Track" signal still embedded in browsers such as Chrome that have yet to enable GPC. Mobile operating systems such as "Limit Ad Tracking" on iOS as well as other IoT platform settings could also be reasonably interpreted as a request not to have data shared or sold under the CPRA. CPRA does not mandate that a request to opt out specifically invoke the CPRA, so any signal from a California resident conveying a request that is roughly equivalent to the right afforded by the statute should be interpreted as legally binding.

c. Clarify that consent to share information despite a general opt-out signal must be specific, informed, and easily withdrawn

Any consent to track notwithstanding a general global privacy control signal has to be clear, specific, and in response to a dedicated prompt. The regulations should also specify that it has to be at least as easy to decline permission as it is to say yes. Moreover, consistent with the CPRA's prohibition on dark patterns[22] and prohibition on retaliation,[23] any such interface must not be coercive or abusive.

For example, the use of vague and unspecific cookie consent notices, originally offered in response to GDPR and the ePrivacy Directive, should not be sufficient to confer consent to sell or share personal information despite a global opt-out signal. Many cookie consent notices conflate consent for both functional and secondary processing, by using design choices that nudge them to accept all processing. For example, we looked at the websites of the 25 top publishers, according to Washington and Lee University, using data from Pew and Comscore,[24] from Los Angeles, California, as simulated by a VPN. The majority of the sites studied have their own separate cookie management interface. California visitors to the *Time* news site, for example, encounter a pop-up:

[21] State of California Department of Justice, CCPA Enforcement Case Examples, "Manufacturer and Retailer Stopped Selling Personal Information," (last visited Nov. 7, 2021), https://oag.ca.gov/privacy/ccpa/enforcement.
[22] Cal. Civ. Code § 1798.140(h).
[23] *Id.* at § 1798.125(a).
[24] Washington and Lee University Library, Top Online News Sites (Summer 2015), https://libguides.wlu.edu/c.php?g=357505&p=2412837.



Clearly, with the red highlighting, the user is encouraged to click on "Accept Cookies[,]" in order to consent to the disclosure of information about their activities on the site with social media, advertising, and analytics companies. The consumer has to click on "Cookie Settings," to ensure that targeting cookies are not permitted. This can hardly be interpreted as an intentional direction to share data. Companies should be encouraged to make it easier for consumers to exercise their preferences, not more difficult.

Even if a company does obtain clear and informed consent to track users notwithstanding a global signal, they must provide opt out links and other easy methods for a user to subsequently

retract such consent. Some have argued that if a consumer agrees to let a business share their personal information, then the business does not have to provide an opt out link for the consumer to stop the sharing or sale of their personal data.[25] The regulations should provide for clear and consistent means for users both to find out whether they have been deemed to provide such consent and how they can easily retract it.

d. Clarify that the sharing opt out applies to retargeting

Many companies have exploited ambiguities in the CCPA's definition of sale and the rules surrounding service providers to ignore consumers' requests to opt out of behavioral advertising.[26] Companies such as Amazon claim that they are not "selling" data and that consumers can't opt out of these data transfers under the CCPA — even though they share it with their advertising partners.[27] Some companies claim that because data is not necessarily transferred for money, it does not constitute a sale.[28] But addressing targeted advertising is one of the main goals of the CCPA.[29] We appreciate that the CPRA clarifies that consumers have the right to opt out of data sharing for the purpose of cross-context targeted advertising,[30] and removes the delivery of cross-context targeted advertising as a business purpose for which businesses could claim an exemption from the opt out.[31] However, more needs to be done to ensure that consumers have adequate protections over this data.

While cross-site behavioral targeting is clearly encompassed by the CPRA's definitions, there remains a hypothetical loophole when it comes to *retargeting*, which is based on a user's activity on just one other site (say, browsing a pair of shoes). While excluding retargeting from the definition of cross-context targeted advertising would be a tendentious stretch — and most

[25] David A. Zetoony, Greenberg Traurig LLC, *Under The CPRA will companies be required to offer consumers the ability to opt-out of behavioral advertising if they have already received opt-in consent?*, NAT'L LAW REVIEW, Volume XI, Number 301 (Oct. 28, 2021), https://www.natlawreview.com/article/under-cpra-will-companies-be-required-to-offer-consumers-ability-to-opt-out.
[26] Maureen Mahoney, *Many companies are not taking the California Consumer Privacy Act seriously—the attorney general needs to act* (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.
[27] "Amazon.com Privacy Notice," (Feb. 12, 2021), https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_FE2374D302994717AB1A8CE585E7E8BE; "Amazon Advertising Preferences" https://www.amazon.com/adprefs.
[28] Tim Peterson, *'We're Not Going to Play Around': Ad Industry Grapples with California's Ambiguous Privacy Law*, DIGIDAY (Dec. 9, 2019), https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/; Tim Peterson, *WTF is California's New, and Potentially Stronger Privacy Law?*, DIGIDAY (July 6, 2020), https://digiday.com/marketing/california-privacy-rights-act/.
[29] Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html; Cal. Civ. Code § 1798.140(o); Cal. Civ. Code § 1798.140(t).
[30] Cal. Civ. Code § 1798.120(a).
[31] *Id.* at § 1798.140(e)(6).

observers have not read the CPRA in this way[32] — others have raised doubts as to whether retargeting is covered under the sharing opt out.[33]

We urge the CPPA to issue clarifying regulations that cross-context targeting based on behavior on just one other site is included within the definition of cross-context targeted advertising. This language will provide much-needed clarity, given the widespread non-compliance and bad faith interpretations of the CCPA with respect to targeted advertising. As AARP points out, "No one likes being followed by an ad, even if we know it's anonymous. It gets even more worrisome when companies that we've given identifiable information to, such as Facebook, Amazon and Google, get involved."[34]

e. Prohibit service providers from combining data

Additionally, the CPPA should clarify that service providers may not combine data across clients. Service providers should be working on behalf of one company at a time. Allowing companies to claim that they are service providers for everyone swallows the rules and lets third parties amass huge, cross-site data sets, allowing them to glean even deeper insights into consumers' most personal characteristics. The CPRA's definition of "service provider" clearly states that a service provider is prohibited from "sharing or selling the personal information" whilst acting as a service provider.[35] Allowing service providers to merge data sets across different clients would run afoul of that provision, as the service provider would effectively be sharing one client's data with another, with itself acting on behalf of both parties.[36]

The CPPA should issue regulations to clarify the intent and purpose of the CPRA's service provider definition. We suggest the following language:

---

[32] 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.
[33] 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.")
[34] Erin Griffith, *Why Is That Ad Following You Across the Web?* AARP, https://www.aarp.org/home-family/personal-technology/info-01-2014/how-to-stop-retargeting-ads.html.
[35] Cal. Civ. Code § 1798.140(ag)(1)(a).
[36] Chris Hoofnagle, *Facebook and Google Are the New Data Brokers* (Dec. 2018), https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf.

A service provider may not combine the personal information which the service provider receives from or on behalf of the business with personal information which the service provider receives from or on behalf of another person or persons, or collects from its own interaction with consumers.

There is precedent for such a prohibition, such as in California's newly adopted SB 41 (Genetic Information Privacy Act), which precludes service providers from combining genetic information received from other clients.[37]

f. Clarify that consumers who have already opted out under CCPA need not resubmit opt-out requests in order to be opted out of data sharing.

Left unaddressed by the statute is whether businesses that have honored consumers' opt out requests under the CCPA are required to automatically opt consumers out of sharing when the CPRA goes into effect in 2023. We urge the CPPA to clarify that businesses must automatically opt such consumers of the sharing of their information when the CPRA goes into effect. Otherwise, consumers would have to identify the companies from which they have already opted out and resubmit, which they are unlikely to be able to do. Moreover, since, as indicated by the recent AG enforcement notice, the existing definition of sale in the CCPA already covers data shared for cross-context targeted advertising,[38] consumers would reasonably expect that they had opted out of such sharing already.

III. Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information

The CPRA provides the right for consumers to limit the use and disclosure of their sensitive personal information, including their financial account information, email, and geolocation data, to what is necessary to provide the service.[39] Particularly since the responsibility falls upon the consumer to ask the business to limit the use and sharing, the protections should be comprehensive and as easy as possible to initiate.

[37] SB 41 at 56.18 (b)(10)(B), (2021), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB41.
[38] State of California Department of Justice, CCPA Enforcement Case Examples, "Media Conglomerate Updated Opt-Out Process and Notices," (last visited Nov. 6, 2021), https://oag.ca.gov/privacy/ccpa/enforcement.
[39] Cal. Civ. Code § 1798.121(a).

a. Clarify that when a consumer limits the use and disclosure of their sensitive information, it is unlawful to process sensitive data for most secondary uses, including monetization, personalization of advertising, and customization of content based on such data.

Especially since the "limit use" right only takes effect upon the consumer's specific request, and since it involves sensitive data, businesses should be very limited indeed in how they are allowed to use such data when "limit use" is enabled. Most secondary uses, including monetization, personalization of advertising, and customization of content should be prohibited when the consumer or their agent has authorized the additional protections.

The ways that ads are targeted — including first-party targeting — can perpetuate historic patterns of discrimination and unequal outcomes among protected classes. For example, the Department of Housing and Urban Development has charged Facebook for targeting housing advertisements based on protected categories like race and religion.[40] Such sensitive information should not be used in determining the advertising and content that consumers view, particularly under "limit use".

Companies should still be allowed to use information to fix errors and engage in fraud prevention, even when "limit use" is enabled, if such use is necessary and proportionate to the purpose.

b. Businesses must honor limit use requests submitted through authorized agents.

The limit use function will only be useful if consumers are able to easily activate it. It only takes effect if the consumer actively requests the use of their sensitive data to be limited, which means that hundreds, if not thousands, of different companies may be using that data without permission. Thus, as outlined in 1798.135(e), businesses must be required to honor requests submitted by authorized agents — consistent with the manner in which opt out requests from authorized agents are processed. Otherwise, it is unlikely that consumers will reap the benefits of this new right.

Authorized agents may be more effective than global controls for these sorts of opt-outs, as first-party uses and relationships vary by context, and individuals may want to be able to exercise nuanced choices as to which parties' uses should be limited. On the other hand, sale and sharing of data generally breaks contextual integrity and consumers who object to such practices (as most do) will likely want to prohibit all parties from engaging in such behavior.

[40] *United States Department of Housing and Urban Development, on behalf of Complainant Assistant Secretary for Fair Housing and Equal Opportunity v. Facebook, Inc*. HUD ALJ No. FHEO No. 01-18-0323-8 https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf; Tracy Jan and Elizabeth Dwoskin, *HUD Is Reviewing Twitter's and Google's Ad Practices as Part of Housing Discrimination Probe*, WASH. POST (Mar. 28, 2019), https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination.

IV. Defining dark patterns

Subverting consumer intent online has become a real problem, and it's important 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.[41] 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.[42] Consumer Reports research has also identified numerous dark patterns, including in smart TV's, food delivery apps, and social media.[43] For example, CR testers found that for all of the smart TVs examined, a consumer moving quickly through the television set-up process will end up providing consent to the tracking of everything they watch through automatic content recognition.[44] And, Consumer Reports is helping to collect dark patterns through the Dark Patterns Tipline, a project to crowdsource examples of these deceptive interfaces to help advocate for reform.[45]

a. <u>The existing prohibition on the use of dark patterns in opt-out processes should be maintained.</u>

We appreciate that the existing CCPA regulations "require minimal steps to allow the consumer to opt-out" and to prohibit dark patterns, "a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out."[46] These regulations are essential given the difficulties that consumers have experienced in attempting to stop the sale of their information.

---

[41] *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.

[42] 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/.

[43] *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/.

[44] *Samsung and Roku Smart TVs Vulnerable to Hacking, supra* note 46.

[45] Dark Patterns Tipline, https://darkpatternstipline.org/.

[46] Cal. Code Regs tit. 11 § 999.315(h).

1. The existing rules appropriately rein in the number of allowable steps to opt out.

We appreciate that the existing rules limit the number of allowable steps in the opt-out process.[47] As we noted in our recent study, some "Do Not Sell" processes involved multiple, complicated steps to opt out, raising serious questions about the workability of the CCPA for consumers. For example, at the time of our study, the data broker Outbrain did not have a "Do Not Sell My Personal Information" link on its homepage (this has since been corrected). The consumer could click on the "Privacy Policy" link at the bottom of the page, which sent the consumer through at least six different steps in order to opt out of the sale of their information on that device. (The consumer could cut out several steps by clicking on "Interest-Based Ads" on the homepage.) As one consumer told us, "It was not simple and required reading the 'fine print.'"[48] Moving forward, the newly-adopted CCPA regulations should help address this problem.

2. The existing rules correctly prohibit companies from asking for unnecessary information to opt out.

We also appreciate the guidance that opt-out processes "shall not require the consumer to provide personal information that is not necessary to implement the request."[49] In our study, the overwhelming reason for a consumer to refrain from part of a DNS request process, or give up altogether, was not feeling comfortable providing information requested. Out of the 68 reports that the tester chose not to provide information they were asked for as part of the process, 59 said it was because they were not comfortable doing so. For example, nearly all consumers declined to provide a photo in order to process their opt-out requests. Out of 7 instances in which consumers reported that they were asked to provide a photo selfie, in 6 the consumer declined.[50]

Consumers told us that they were just as averse to providing government IDs. One tester of Searchbug reported: "I hated having to send an image of my Driver License. I thoroughly regret having done so. It feels like an invasion of privacy to have to do that, just so I can take steps to PROTECT my privacy. Feels wrong and dirty."[51] Even consumers that ended up providing the drivers' license ended up confused by the company's follow-up response. One tester of Hexasoft Development Sdn. Bhd. responded: "After sending them a copy of my California driver license to satisfy their residency verification, I got an email back which simply stated that '[w]e will update the ranges in the future release.' I have no idea what that means."[52] Out of 17 reports of being asked for an image of a government ID, in 10 the consumer chose not

[47] *Id*. at § 999.315(h)(1).
[48] *Are Consumers' Digital Rights Protected?*, *supra* note 8, at 18-21.
[49] Cal. Code Regs tit. 11 § 999.315(h)(4).
[50] *Are Consumers' Digital Rights Protected?*, *supra* note 8, at 34.
[51] *Id*.
[52] *Id*.

to. Out of 40 reports of being asked to provide a government ID number, in 13 the consumer refrained from providing it.[53]

This information is clearly not necessary, as most data brokers simply requested name, address, and email to process opt outs (where authentication is not required). Unnecessary collection of sensitive data has significantly interfered with consumers' ability to exercise their rights under the CCPA, and we appreciate that the newly-adopted CCPA rules explicitly prohibit this.

3. The existing rules correctly stop businesses from making consumers search through a privacy policy to opt out.

We are also pleased that the existing rules preclude businesses from requiring consumers to dig through privacy policies to opt out.[54] In our study, in some cases, consumers proactively reported finding language surrounding the DNS request link and process excessively verbose and hard to understand. For example, one tester reported of the data broker US Data Corporation, "There is a long, legalistic and technical explanation of how and why tracking occurs, not for the faint of heart." Another said of Oracle America, "The directions for opting out were in the middle of a wordy document written in small, tight font." Another found the legal language used by Adrea Rubin Marketing intimidating: "they seemed to want to make the process longer and unnecessarily legalese-y, even a bit scary--under threat of perjury."[55]

b. Clarify that companies that sell personal information must post the opt out button to their homepages, along with the "Do not Sell My Personal Information" link.

We appreciate that the existing rules include a logo, or button, for companies that sell personal information to post alongside the "Do Not Sell My Personal Information" link on the homepage.[56] However, unless use of the button is required, it is unlikely that companies will adopt it. While we think it is clear that the language in § 999.306(f)(1)-(3) requires companies selling personal information to post the button on their homepages, some observers have a different interpretation, that posting of the button is optional.[57] And in fact, the authors have yet to encounter a website in which this graphic is used. An optional interface counters the direct instructions in the CCPA, to issue rules "For the development and use of a recognizable and

[53] *Id.*
[54] Cal. Code Regs tit. 11 § 999.315(h)(5).
[55] *Are Consumers' Digital Rights Protected?*, *supra* note 8, at 32.
[56] Cal. Code Regs tit. 11 §999.306(f)(1)-(3).
[57] See, eg, @JulesPolonetsky, Twitter (Dec. 10, 2020), https://twitter.com/JulesPolonetsky/status/1337116699548667907.

uniform opt-out logo or button *by all* businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information."[58] [emphasis added]

To help eliminate any uncertainty that the opt out button is required, we propose the following tweak to the language:

> Opt-Out Button. (1) The following opt-out button ~~may~~ shall be used in addition to posting the notice of right to opt-out, ~~but~~ and not in lieu of any requirement to post the notice of right to opt-out or a "Do Not Sell My Personal Information" link as required by Civil Code section 1798.135 and these regulations. (2) Where a business posts the "Do Not Sell My Personal Information" link, the opt-out button shall be added to the left of the text as demonstrated below. The opt-out button shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" link. (3) The button shall be approximately the same size as any other buttons used by the business on its webpage.

Without more clearly establishing that use of the opt-out button is required on the homepage, it is likely that companies continue to disregard it. Standardized notice is essential to making CCPA disclosures meaningful and understandable for consumers and to limiting company's discretion to craft less clear or useful interfaces. And widespread adoption of the button should better ensure that consumers can more easily opt out of the sale of their personal information.

c. Develop a standardized opt-in interface to help prevent dark patterns in obtaining consent.

The CPPA should also develop standardized disclosures, so that companies have more clarity about appropriate interfaces and design choices. As discussed above, we appreciate that the CCPA requires rulemaking entities to create a uniform Do Not Sell logo[59] — this standardization can help companies avoid dark patterns (if, as we recommend, the CPPA makes clear that use of the button is required).[60]

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 the sharing or sale of children's

[58] Cal. Civ. Code § 1798.185(a)(4)(C).
[59] *Id.*
[60] See, for example, Cranor et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* (Feb. 4, 2020), https://cups.cs.cmu.edu/pubs/CCPA2020Feb04.pdf.

information. Overall, the CPPA should err strongly on the side of clear, simple, bright-line rules instead of vague, debatable standards that could afford bad faith actors too much wiggle room to justify deceptive behavior.

V. Automated decision-making

As automated decision-making that uses artificial intelligence is on the rise for commercial applications like determining housing and employment eligibility, facial recognition, and even software for self-driving cars, the potential to perpetuate existing societal inequalities is worrying. AI models are trained on data that tends to represent historical outcomes (for example, hiring algorithms compare applicants to those who currently hold positions at a given company which can tend to exclude minorities and women). Many of these algorithms (intentionally or unintentionally) could be used to discriminate against groups of people that have historically been excluded from services or opportunities in the past.[61] Also, some companies claim that correlations between unrelated data can predict behavior or other outcomes, with little evidence, often leading to discriminatory results.[62]

Further, some of these algorithms are black boxes to both the end-users as well as the engineers that design them. Establishing appeals processes or other pathways to provide opportunities for individuals to correct data about themselves becomes less meaningful when there are thousands of data points and opaque models and results.

It will be close to impossible to entirely rid algorithms of bias,[63] but pursuant to the CPRA, which directs the Agency to develop rules providing opt out and access rights with respect to automated decision-making,[64] the CPPA can put guardrails in place to mitigate or prevent harmful effects of discrimination.

a. <u>Require increased transparency measures from companies designing algorithms with significant legal effects</u>

While there are laws that prohibit discrimination based on certain characteristics for various sectors, due to the opacity of more complicated algorithms, it is difficult to tell whether algorithmic discrimination is occurring at all. There are virtually no laws, other than CPRA, that require companies to disclose how their algorithms work, the types of data they use to make decisions, or mandate providing ways for consumers to contest decisions made about them. For

[61] Nandita Sampath, *Racial Discrimination in Algorithms and Potential Policy Solutions* (Feb. 26, 2021), https://medium.com/cr-digital-lab/racial-discrimination-in-algorithms-and-potential-policy-solutions-75c5911ed29.
[62] Arvind Narayanan, Princeton University, *How To Recognize AI Snake Oil*, https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf.
[63] Chris Caruso, *Why AI Will Never be Perfect* (Sept 28, 2016), https://medium.com/@chriscaruso/why-ai-will-never-be-perfect-c34aec481048.
[64] Cal. Civ. Code § 1798.185(a)(16).

decision-making involving significant legal effects, consumers deserve transparency. We advise that for algorithms with significant legal effects (including housing, credit/lending, insurance, employment), meaningful transparency measures need to be created in order to identify and mitigate discrimination. Section 21(a)(16) allows the Agency to issue regulations governing access and opt-out rights. To facilitate this, at the very least, companies should be required to provide notice in its privacy policy that algorithms are being used to make significant decisions about them to provide some degree of transparency and accountability.[65]

Companies often use multiple data points that are fed into the algorithm to make a decision about how a consumer behaves, and companies should be required to provide all of that data access requests. Companies should be required to disclose the types of data collected, the specific data that it has on the consumer in order to profile them, and how each data point is factored into the final algorithmic decision (to the extent possible), pursuant to access requests.[66] For example, if a particular data point holds more weight in a decision, the consumer should be informed and given a quantitative value if possible. In order to give consumers this information in a meaningful way, companies should use more transparent and interpretable algorithms and avoid using algorithms that tend to be more complicated to understand like neural networks.

For housing and employment-related targeted advertising, discrimination based on protected classes including race, gender, religion, etc. is prohibited.[67] Consumers deserve transparency as to why certain ads are shown to them which should include providing consumers with meaningful information when the consumer requests it. For example, some companies like Facebook provide users with the option to learn more about why they see certain ads. However, the information is often overly broad and generalized, with explanations like "interests" or "offline activity."[68] For targeted ads with the potential of significant legal effects, consumers should be shown how ads are targeted to them with improved specificity.

For other sensitive algorithms like determining insurance premiums, companies should also disclose *why* data points that are factored into the algorithms were chosen, provide explanations for ways consumers can improve their algorithmic "risk score," and also make sure consumers have the ability to contest inaccurate data about themselves. This requires that consumers have easy access to real-time information about themselves that can be accessed without hurting their score and also requires a straightforward process to contest inaccurate

---

[65] *Invitation for Comments*, *supra* note 2, at 2(b) and 2(d).
[66] Under Cal. Civ. Code § 1798.185(21)(a)(16), the Agency has the authority to require businesses to provide meaningful information about the algorithm's logic and the outcome of the process.
[67] Ava Kofman & Ariana Tobin, *Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement*, PRO PUBLICA (Dec. 13, 2019), https://www.propublica.org/article/facebook-ads-can-still-discriminate-against-women-and-older-workers-despite-a-civil-rights-settlement.
[68] *Why Am I Seeing Ads From An Advertiser at Facebook?,* Facebook.com Help Center (last visited Nov. 1 2021), https://www.facebook.com/help/794535777607370.

information that must be corrected in a timely manner (or be provided a clear explanation as to why the data is not inaccurate).

b. Identify and ban pseudoscience in AI and other egregious algorithmic harms

There are certain harmful applications of AI where improved transparency and better consumer control of data are not enough, and should be prohibited. Some AI companies claim that their technology is capable of doing certain things that are not substantiated by science or claim certain accuracy rates of their technology without third-party validation.[69] Under Section 21(a)(15), the Agency has the authority to require businesses to submit risk assessments weighing consumer harm with the processing of their personal information, "with the goal of restricting or prohibiting such processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public."[70] And some of these pseudoscientific algorithms can cause real harm.

In the employment space, companies like HireVue have been criticized for building video interviewing software that claims to rank job applicants based on the tone of their voice and facial expressions. There is little evidence that these factors are related to job performance; more importantly, these kinds of algorithms have the potential to discriminate against those with certain skin colors, accents, or disabilities.[71] Generally, using AI to predict subjective processes like job success, recidivism, etc. will result in discriminatory outcomes; trying to quantify subjective processes where the goals might be different depending on who designs the AI system tends to hurt those historically marginalized. While unfair and deceptive practices are outlawed at the state and federal levels, the CPPA needs to make more clear what kinds of AI applications fall under this category.

c. Design an accreditation system for private auditing companies to perform audits on algorithms with significant legal effects

Third-party auditing can be an effective way to mitigate disparate impacts and other algorithmic harm. Pursuant to Section 21(a)(18), which directs the Agency to establish regulations with respect to auditing companies, including identifying criteria for selection of entities to audit, the Agency should design an accreditation system for companies that use AI that ensures accountability.[72] It is important to ensure that audits performed on different companies' AI are done in a standardized and stringent manner. There are virtually no industry-wide or legal

[69] Narayanan, *supra* note 65.
[70] Enforcement against unsubstantiated claims in AI can also be pursued by the Attorney General under California's Unfair Competition Law.
[71] Drew Harwell, *Rights Group Files Federal Complaint Against AI-Hiring Firm HireVue, Citing 'Unfair and Deceptive' Practices*, WASH. POST (Nov. 6, 2019), https://www.washingtonpost.com/technology/2019/11/06/prominent-rights-group-files-federal-complaint-against-ai-hiring-firm-hirevue-citing-unfair-deceptive-practices/.
[72] Cal. Civ. Code § 1798.185(a)(18).

standards for what kinds of information companies should be providing to auditors about their technology in order for an audit to take place, and even what the audit should be addressing. Considering AI applications are diverse and varied, these standards need to be nuanced based on the technology's impact.

Certain private auditing companies market their auditing services to AI companies in the hopes of mitigating some potential harm. However, since there are no legal requirements for a third-party audit in most cases, the incentive structure here is skewed in a way that may not be optimal for unbiased and robust testing. Companies that voluntarily undergo auditing may be doing it as a PR stunt, either to push back against criticism of their product or to attempt to show some kind of transparency.[73] Furthermore, due to the lack of requirements in making the results of audits public, companies can cherry-pick and publish the positive attributes of their audit results while withholding the auditors' acknowledgement and assessment of any potential harms.

Since there are generally no real requirements for companies to have to undergo an audit at all, AI companies likely have a decent amount of leverage in terms of what types of audits they want to undergo, what specific algorithms they want to be audited, and how much of their information they want to give to auditors (even under an NDA). The incentive structure here is clearly skewed towards AI companies that in most cases do not legally need the services of these auditors. Furthermore, as the number of auditing companies increase, they will likely be competing on a basis of audits that are most comfortable and convenient for AI companies, reducing some of the potential benefits that a stringent and standardized audit can provide. It is also likely that different auditing companies have wildly different techniques in terms of which biases/issues they search for and how they go about identifying them — Auditor A might obtain a significantly different impact assessment of a company's algorithm than Auditor B. Finally, the results of these audits are not usually something companies legally need to address if there is indeed a problem.

Overall, there is a lack of industry and legal standards for what an audit should be composed of, what issues of bias and other harm need to be addressed, and what kinds of information about the technology companies need to provide to auditors to carry out the audit. There is also a lack of transparency requirements regarding how the results of these audits should be released to the public (if at all) and, most importantly, how companies need to address the results of the audit.

We recommend that the CPPA design an accreditation system for private auditing companies, require companies that deploy algorithms with significant legal effects (including but not limited to housing, employment, insurance, credit/lending) undergo audits, and establish

[73] Alfred Ng, *Can Auditing Eliminate Bias from Algorithms?* THE MARKUP (Feb. 23, 2021), https://themarkup.org/ask-the-markup/2021/02/23/can-auditing-eliminate-bias-from-algorithms.

what audits for particular applications should consist of and what information companies must disclose to auditors about their technology. The Agency should also require that auditors disclose the results of a company's audit if discrimination based on a protected class is identified and the company has not been able to mitigate the issue within a specified period of time.

VI. Consumers' Right to Correct

Studies of the credit reporting error reinvestigation process under the Fair Credit Reporting Act (FCRA) can be instructive with respect to error correction under CPRA.[74] Credit reporting errors are pervasive — in a recent Consumer Reports study, 34% of participants found at least one error on one of their credit reports.[75] Under the FCRA, when a consumer reports an error, consumer reporting agencies (CRAs) have a legal responsibility to investigate the issue fully.[76] But the automated system developed by the CRAs to resolve disputes does not always adequately address consumer complaints. The dispute investigation system places much of the power to adjudicate the dispute into the hands of the data furnisher, which often performs just a cursory investigation.[77] With respect to the CPRA's requirement to "use commercially reasonable efforts to correct the inaccurate personal information" about a consumer,[78] and pursuant to the Agency's authority to develop regulations with respect to businesses' responses to correction requests,[79] we recommend adopting regulations that help address these potential issues under CPRA.

---

[74] Syed Ejaz, *A Broken System: How the Credit Reporting System Fails Consumers and What to Do About It*, CONSUMER REPORTS (Jun. 10, 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/06/A-Broken-System-How-the-Credit-Reporting-System-Fails-Consumers-and-What-to-Do-About-It.pdf; Chi Chi Wu et al., *Automated Injustice Redux: Ten Years After a Key Report, Consumers Are Still Frustrated Trying to Fix Credit Reporting Error*s, NAT'L CONSUMER LAW CTR. (Feb. 2019), https://www.nclc.org/images/pdf/credit_reports/automated-injustice-redux.pdf. NCLC has found that despite significant credit reporting reforms over the course of the last decade, serious problems with the credit reporting dispute process remain; *Key Dimensions and Processes in the U.S. Credit Reporting System: A review of how the nation's largest credit bureaus manage consumer data*, CONSUMER FIN. PROTECTION BUREAU (Dec. 2012), https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf; Chi Chi Wu, *Automated Injustice: How a Mechanized Dispute System Frustrates Consumers Seeking to Fix Errors in their Credit Reports*, NAT'L CONSUMER LAW CTR. (Jan. 2009), https://www.nclc.org/images/pdf/pr-reports/report-automated_injustice.pdf; Maureen Mahoney, *Errors and Gotchas: How Credit Report Errors and Unreliable Credit Scores Hurt Consumers*, CONSUMERS UNION (2014), https://advocacy.consumerreports.org/research/errors-and-gotchas-how-credit-report-errors-and-unreliable-credit-scores-hurt-consumers/.

[75] *A Broken System*, *supra* note 77, at 4.

[76] 15 U.S.C. § 1681(a)(1)(A).

[77] See, e.g., Chi Chi Wu, *Automated Injustice*, *supra* note 77, at 21-25; *Key Dimensions*, *supra* note 77, at 35.

[78] Cal. Civ. Code § 1798.106(a).

[79] *Id.* at § 1798.185(a)(8)(A).

a. Businesses should be required to delete disputed information if it cannot provide documentation to back it up.

In ensuring that consumers are able to correct inaccurate information pursuant to CPRA,[80] and in developing rules on businesses' responses to correction requests,[81] the CPPA should direct companies to delete disputed information that cannot be backed up with documentation. With respect to credit reporting, the CRAs and furnishers primarily rely on an automated online system known as e-OSCAR to transmit information about disputes to one another, and to resolve them.[82] However, it does not always serve the best interests of consumers. First, CRA call center agents have often not been equipped to provide consumers with the help they need. In 2013, Experian call center agents in Santiago, Chile revealed that they had no power to actually investigate error complaints, but merely to code the disputes, and accept the account of the furnisher.[83]

The CRAs allow the furnishers a great deal of power in conducting the investigations and determining whether or not an error has occurred. The CRAs often take the word of the furnisher in handling these complaints. This is problematic for consumers for two reasons. First, this unfairly places the responsibility on the consumer to show that the furnisher has made a mistake.[84] FCRA requires CRAs to remove any information from a report that "cannot be verified," thus furnishers have the responsibility to prove the consumer wrong.[85] Second, furnishers often fail to conduct a thorough investigation into the problem, which raises questions about the veracity of their claims in some cases.[86]

Furnisher investigations are inadequate to correct many types of errors. According to an industry source, attorney Anne P. Fortney, a typical furnisher investigation had the employee "at a minimum, verify the consumer information by matching the name, Social Security number and other pertinent data; and review the account history, including payment history and any historical notes related to the account."[87] These investigations can be lacking, especially when the errors

[80] *Id.* at § 1798.106(a).
[81] *Id.* at § 1798.185(a)(8)(A)
[82] Report to Congress on the Fair Credit Reporting Act Dispute Process, FED. TRADE COMM'N at 15 (2006), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-andboard-governors-federal-reserve-system-report-congress-faircredit/p044808fcradisputeprocessreporttocongress.pdf; e-OSCAR, www.e-oscar.org.
[83] *Steve Kroft, 40 Million Mistakes: Is Your Credit Report Accurate?*, CBS NEWS (Aug. 25, 2013), http://www.cbsnews.com/news/40-million-mistakes-is-your-credit-report-accurate-25-08- 2013/ (60 Minutes broadcast originally aired on Feb. 10, 2013) (see 2 of transcript).
[84] *Automated Injustice*, *supra* note 77, at 28.
[85] 15 U.S.C. § 1681i(a)(5)(A).
[86] *Automated Injustice Redux*, *supra* note 77, at 14-15.
[87] Credit Reports: Consumers' Ability to Dispute and Change Inaccurate Information: Hearing Before the H. Comm. on Fin. Servs., 110th Cong. (2007) (statement of Anne P. Fortney), http://archives.financialservices.house.gov/hearing110/osfortney061907.pdf (see 9 of PDF).

were already caused by or reflected in the furnisher's computer records. In other cases, it is clear that the employees in charge of the reinvestigation fail to uphold even these minimum standards.

Many courts have found that the existing procedures CRAs and furnishers use fall short of what constitutes a "reasonable" investigation as required by FCRA. For example, In *Dickman v. Verizon Communications, Inc.* (2012), the court refused to dismiss the case against Verizon and found that there were questions about the adequacy of their investigation process in part because, as the plaintiff argued, Verizon informed the CRAs "that he had become delinquent on the [n]ew [a]ccount three months before he actually opened it."[88] This error revealed that Verizon had not fully investigated the error complaint, since it supplied information that was clearly false. Verizon claimed that it followed a similar procedure as described by Fortney to investigate errors —checking the account, verifying the name and other identifiers, and looking at the record of past payments.[89]

In *Boggio v. USAA Federal Savings Bank* (2012), USAA employees responded to an error complaint by simply reconfirming the plaintiff's identity, and did not review any underlying documentation in his file.[90] The court denied USAA's motion for summary judgment in their favor because it could not conclude that USAA's investigation was "reasonable" as a matter of law.[91] The plaintiff sued because he believed he was incorrectly listed as a "co-obligor" on his ex-wife's loan—information that had been forwarded to the CRAs.[92] Deposition testimony revealed that USAA employees are "not permitted to make any phone calls to anyone" or review any documents submitted by paper.[93]

Dixon-Rollins v. Experian Information Solutions, Inc. (2010) revealed that TransUnion and furnishers did not conduct a reasonable investigation of the plaintiff's dispute as required by law.[94] The court upheld the judgment and award for the plaintiff, finding that TransUnion had not fulfilled its duty to investigate in part because it did not forward any of the documentation that plaintiff Dixon-Rollins provided to the debt collector during the reinvestigation, and simply accepted the debt collector's word.[95] Although Dixon-Rollins had paid off the debt, her four attempts to have the incorrect information altered on her credit report were in vain.[96] The debt

[88] 876 F.Supp.2d 166, 174 (E.D.N.Y. 2012).
[89] *Id.* at 173.
[90] 696 F.3d 611, 619 (6th Cir. 2012).
[91] *Id.* at 619-20.
[92] *Id.* at 613.
[93] Brief for Appellant, Boggio v. USAA Fed. Sav. Bank, 696 F.3d 611, 2012 WL 248111, at *8 (6th Cir. 2012) (No. 11-4040.)
[94] Dixon-Rollins v. Experian Info. Solutions, Inc., 753 F. Supp. 2d 452, 465 (E.D. Pa. 2010) (defendant "repeatedly failed to carry out its statutory duty" under FCRA). The plaintiff sued both Experian and TransUnion, but reached a settlement with Experian. *Id.* at 456.
[95] *Id.* at 456-7, 459. The award was reduced, however. Id. at 456.
[96] *Id.* at 457.

collector simply checked its records and reconfirmed to the CRA— incorrectly—that the debt had not been paid.[97]

These examples help to demonstrate how minimal steps taken by CRAs and furnishers do not always properly address or even clarify the underlying dispute. In many cases, CRAs have accepted the word of the furnisher, even when they don't have evidence to back up their case. This is true even for disputes from furnishers who are debt collectors. CRAs have accepted a furnisher's response to the dispute, even if the consumer is actually correct, has documentation that she is correct, and the furnisher has sent nothing to back up its response. The National Consumer Law Center notes that this not only places the burden of proof on the consumer, it unfairly gives the furnisher the role of being the judge in the dispute against it.[98]

Therefore, to ensure that consumers are able to correct inaccurate information pursuant to CPRA, the agency should direct companies to delete disputed information that cannot be backed up with documentation. Businesses should not simply accept the word of the data provider in a dispute without any evidence. Disputed information should be removed from a consumer's record if the provider is unable to provide documented proof of its claims following a consumer dispute.

b. <u>Businesses should delete challenged information that they cannot link to a single identifiable consumer.</u>

In developing rules on businesses' responses to correction requests,[99] the agency should direct companies to delete disputed information when it cannot be linked to a single identifiable consumer. So-called "mixed files" — in which information from multiple people, often family members with similar names and the same address, is pulled into a single credit report — are a common source of credit reporting mistakes.[100] The case of Miller v. Equifax Information Services LLC (2013)[101] highlighted some of these lapses in the CRA investigation system, especially when trying to correct a mixed file. In this case, the court upheld the judgment and granted Julie Miller $1.8 million in both punitive and compensatory damages after Equifax ignored her efforts to remove errors from her credit report.[102] Over the course of two years, Miller challenged a number of collections entries on her credit report that did not belong to her,

[97] *Id.*
[98] Making Sense of Consumer Credit Reports: Hearing Before the Subcomm. on Fin. Inst. and Consumer Protection of the Sen. Comm. On Banking, Housing and Urban Affairs, 112th Cong. (2012) (statement of Chi Chi Wu, NCLC), available at http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=1b5d9716-9a48-4757-90d8-7a69d33af0ca (see 22-24 of PDF).
[99] *Id.* at § 1798.185(a)(8)(A)
[100] *Automated Injustice Redux*, *supra* note 77, at 13-14.
[101] No. 11-1231 (D. Or. Jan. 29, 2014).
[102] Miller, No. 11-1231, slip. op. at 2. At trial, the jury had granted $18 million. Id.

but Equifax failed to remove them.[103] Equifax's representative testified that while she couldn't conclusively explain the reason for this lapse, Equifax employees may have let the marks remain because they couldn't verify the plaintiff as the owner of the credit file.[104] Although Equifax maintained that it established special procedures to deal with a mixed file, in this case, standard procedures were not followed.[105]

These mixed files are likely to be even more common with respect to information held by data brokers, since information, such as about browsing history, could likely be linked to all consumers that use a particular device. Thus, businesses should delete challenged information that they cannot link to a single identifiable consumer.

c. Businesses should be required to review correction requests in which the consumer submits new information that is relevant to the complaint, unless the request appears to be vexatious or in bad faith.

Given the challenges that consumers have experienced in correcting credit reporting errors, it is likely that they will encounter similar problems in correcting errors under the CCPA. With respect to the new correction rights under the CPRA, the CPPA has authority to establish "[H]ow often, and under what circumstances, a consumer may request a correction" of their personal information.[106] Consumers should be permitted to submit additional documents or evidence in support of their dispute, without having to worry that the dispute will be marked "frivolous" and dismissed. Such dismissals occur all too often in credit reporting disputes.[107] Thus, companies should be required to consider new information and documentation provided to them by consumers even in an ongoing dispute, as long as it is relevant to the complaint.

Of course, if a bad actor were attempting to interfere with the functioning of the service by sending hundreds of requests per day, it would be reasonable just to ignore these bad-faith requests and not look up the consumer's file each time.

[103] Complaint at 6, Miller v. Equifax Info. Servs., No. 11-1231 (D. Or. Jan. 29, 2014); see also Laura Gunderson, *Equifax Must Pay $18.6 Million After Failing to Fix Oregon Woman's Credit Report*, THE OREGONIAN (July 26, 2013), http://www.oregonlive.com/business/index.ssf/2013/07/equifax_must_pay_186_million_a.html (noting that the Miller judgment would be the largest award ever obtained in a case against a major CRA).
[104] Transcript of Record at 278-84, Miller v. Equifax Info. Servs., No. 11-1231 (D. Or. Jan. 29, 2014).
[105] *Id*. at 442-47.
[106] Cal. Civ. Code § 1798.185(a)(8).
[107] *Automated Injustice Redux*, *supra* note 77, at 21-22.

VII. Consumers' Right to Know

a. In response to a verifiable request, businesses should be required to provide all information that belongs to that identifiable consumer, even if it is beyond the 12-month window.

Businesses should not reidentify information in order to respond to an access request. But if the company has identifiable data, it should provide that data to the consumer or their authorized agent pursuant to an access request, even if the data is older than 12 months.[108] Since this access requirement applies only to data collected on or after January 1, 2022,[109] and businesses have been required to comply with access requests since 2020, they will have had ample time to prepare to respond to such requests.

If a company collects and retains a consumers' personal information, at the very least, they should give the consumer the ability to access that information. These access rights are necessary for consumers seeking to take additional action to exercise their portability and correction rights. Further, the information consumers receive through such access requests may cause them sufficient concern that they then decide to delete or stop the sale of this information.

And businesses should be incentivized to get rid of old data. Retaining old and unnecessary data is a serious security risk; a recent data breach at Capital One involved data that was more than ten years old.[110] Exempting old data from access requests doesn't help businesses or consumers when there is such a threat of inadvertent disclosure. The CCPA changed the incentive structure for maintaining data: companies that previously had no reason to map data finally had to do so in order to be prepared to respond to requests — leading some of them to delete old data that was no longer needed.[111] But unless companies are held to the requirement to honor access requests with respect to data that is more than a year old, companies will have fewer incentives to do so.

Finally, the CPRA requires companies to delete data that is no longer necessary for disclosed purposes,[112] so it should not be too burdensome for companies to respond to access requests for the remaining data.

---

[108] Cal. Civ. Code § 1798.185(9).
[109] *Id.* at § 1798.130(a)(2)(B).
[110] Emily Flitter and Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, N.Y. TIMES (Jul. 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.
[111] Kaveh Waddell, *California Privacy Law Prompts Companies to Shed Consumer Data*, CONSUMER REPORTS (Feb. 11, 2020), https://www.consumerreports.org/privacy/california-privacy-law-ccpa-prompts-companies-to-shed-consumer-data-a8999779184/.
[112] Cal. Civ. Code § 1798.100(3).

VIII. Non-Discrimination

Californians have a right to privacy under the California Constitution, and consumers should not be charged for exercising those rights.[113] Unfortunately, there is contradictory language in the CCPA, including as amended by CPRA, that could give companies the ability to charge consumers more for opting out of the sale of their data or otherwise exercising their privacy rights.[114] We offer several recommendations to help ensure that these loopholes are not inappropriately exploited.

a. The CPPA should clarify that financial incentives in markets that lack competition is an unfair and usurious practice.

To prevent some of the worst abuses associated with financial incentives, discriminatory treatment should be presumed where markets are consolidated and consumers lack choices. The CCPA prohibits financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.[115] And, the CPPA currently has the authority under CPRA to issue rules with respect to financial incentives.[116] Thus, we urge the CPPA to exercise its authority to prohibit the use of financial incentives in market sectors that lack competition. ISPs, for example, should not be allowed to charge consumers for exercising their privacy rights, because customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged usurious rates — about $30 per month — for not leveraging U-Verse data for ad targeting.[117] Where consumers have few choices, market forces don't impose sufficient constraints on companies from penalizing exercising privacy rights. And, there is rising concentration across many industries in the United States,[118] further highlighted by the creation of a Federal Trade Commission task force to monitor these trends.[119] The CPPA should exercise its authority to put reasonable limits on these programs in consolidated markets.

---

[113] Cal. Cons. § 1, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I.
[114] Cal. Civ. Code §§ 1798.125(a)(2) and .125(b).
[115] *Id.* at § 1798.125(b)(4).
[116] *Id.* at § 1798.185(a)(6).
[117] Jon Brodkin, *AT&T To End Targeted Ads Program, Give All Users Lowest Available Price*, ARS TECHNICA (Sept. 30, 2016), https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/.
[118] *Too Much of a Good Thing*, THE ECONOMIST (March 26, 2016), https://www.economist.com/briefing/2016/03/26/too-much-of-a-good-thing.
[119] *FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets,* FED. TRADE COMM'N (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

b. Businesses must calculate the value of the data to the business and make it available per access requests before being permitted to share data with third parties pursuant to loyalty programs.

Under the existing CCPA regulations, companies that provide financial incentives to consumers that could implicate their CCPA rights are required to give notice, including "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[.]"[120] However, a check of two top loyalty programs suggests that too many companies aren't taking this requirement seriously, offering only vague explanations in their disclosures with respect to the value of consumers' data.[121]

The CPPA should carry over the prohibition on discrimination if a company cannot meet the affirmative burden of offering a good faith estimate and demonstrating that a financial incentive is reasonably related to the value of the data. It should specifically extend that idea to loyalty programs, to prohibit secondary sharing unless a company can meet those two evidentiary burdens.

IX. Conclusion

We thank the CCPA 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 Maureen Mahoney (maureen.mahoney@consumer.org) for more information.

[120] Cal. Code Regs tit. 11 § 999.307(b)(5)(a).
[121] See, for example, 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[,]" (Nov. 1, 2021), https://www.sephora.com/beauty/privacy-policy#USNoticeIncentive; CVS, Privacy Policy, Financial Incentives, Member Special Information, "The value we place on the personal information in connection with these incentives is calculated by determining the approximate additional spending per customer, per year compared to individuals who are not enrolled in ExtraCare[,]" (Sept. 16, 2021), https://www.cvs.com/help/privacy_policy.jsp#noticefi.