Comments of Consumer Reports
In Response to the
Colorado Attorney General's Office
Request for Comments Pursuant to
Proposed Rulemaking under the Colorado Privacy Act

by

Justin Brookman, Director of Technology Policy
Nandita Sampath, Policy Analyst

August 5, 2022

Consumer Reports[1] appreciates the opportunity to provide preliminary comments on the proposed rulemaking under the Colorado Privacy Act (CPA).[2] We thank the Colorado Attorney General's office for soliciting input to make the CPA most effective for consumers.

I. UNIVERSAL OPT-OUT MECHANISMS

Universal opt-out mechanisms (UOOMs) 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 (CCPA) 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.[3] As consumers cannot practically opt out at every one of the hundreds, if not thousands, of companies that sell consumer data, the Attorney General must provide clarity as to how companies should adhere to UOOMs to make the exercise of consumer rights meaningful for Colorado citizens.

A. UOOM registry

The Attorney General should create and regularly update a list of signals and settings that should be treated as legally binding requests under the CPA. The Global Privacy Control, a web-based UOOM with over 50 million unique users each month, should be one of the UOOMs designated as conveying a legally binding request to opt out of the sharing or selling of a user's personal information under § 6-1313(2).[4] The Global Privacy Control was the first global opt-out signal recognized by the California Attorney General as legally binding under the CCPA.[5] The Attorney General 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 sold or used

---

[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] Colorado Privacy Act (CPA) Rulemaking, Phil Weiser, Colorado Attorney General, https://coag.gov/resources/colorado-privacy-act/.

[3] 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.

[4] 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.

[5] California Consumer Privacy Act, Frequently Asked Questions, https://oag.ca.gov/privacy/ccpa.

for targeted advertising under the CPA. Similar controls on other platforms such as Smart TVs should also be evaluated to determine if they are consistent with the CPA's requirements. The CPA does not mandate that a request to opt out specifically invoke §§ 6-1-1306(1)(a)(I)(A) or (1)(a)(I)(B), the terms "targeted advertising" or "sale," or even the CPA, so any signal from a Colorado resident conveying a request that is roughly equivalent to the right afforded by the statute should be interpreted as legally binding (*see infra*, § I.B (scope and definitions).

As new UOOMs are added to the list, the Attorney General 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.

B. Scope and definitions

Section 6-1-1313(2) states that UOOMs may apply to either the sale of personal information or the use of personal information for targeted advertising. In practice, these rights will significantly overlap, and consumers are unlikely to always understand the nuances of which behaviors and data sharing practices are covered by which right. To make privacy choices simpler for Colorado consumers, by default, UOOMs should be interpreted as invoking both rights, unless an UOOM is specifically promoted as limited to just one opt-out right. This would allow Colorado's law to be interoperable with California and other emerging state privacy laws, all of which define opt-out rights slightly differently (the CPRA, for example, allows consumers to opt out of "sharing," including for the purposes of "cross-context targeted advertising"). UOOMs should not have to articulate a sprawling 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 UOOM.

To ensure that UOOMs work for consumers as intended, the Attorney General should also provide clarity about the scope of the terms "sale" and "targeted advertising" to ensure that companies cannot adopt tendentious interpretations to avoid the law's interpretation. For example, the term "targeted advertising" is defined as:

> displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests.

This definition introduces a potential ambiguity 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 targeted advertising would be contrary to the spirit of the law — and most observers have not read similar language contained in the CPRA in this way[6] — others have raised doubts as to whether retargeting is covered under the CPRA's sharing opt out.[7] Exempting retargeting — arguably the prototypical example of targeted advertising — from the scope of targeted advertising would frustrate consumers and offer a gaping loophole that cross-context marketers could take advantage of; the Attorney General should specify that targeted ads based on even one nonaffiliated website, application, or online service is still a targeted ad.

Similarly, many companies in response to the CCPA adopted interpretations of the terms "sale" and "service provider" to ignore consumers' requests to opt out of sharing related to ad targeting.[8] Companies such as Amazon have claimed that they are not "selling" data and that therefore consumers could not opt out of these data transfers under the CCPA — even though the data was shared with their advertising partners.[9] Some companies have claimed that the data itself is not necessarily transferred for consideration — instead, it was the underlying ad space that was sold and the data was only used to target the ad.[10] The Interactive Advertising Bureau seemingly blessed this interpretation, and also suggested that companies could designate

---

[6] *See*, *e.g.*, *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.

[7] *See* 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.")

[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] 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.

[10] 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/.

advertising partners to be "service providers" and thus outside the scope of the law's opt-out rights.[11]

Advertisers may attempt to exploit similar loopholes in comparable definitions under the CPA to continue data sharing and targeting practices despite consumer attempts to opt out. The definition of sale under the previous version of the CCPA and the current CPA are similar (the CCPA was amended by the CPRA to close this loophole, and Attorney General Bonta has issued enforcement letters disputing companies' narrow interpretation of "sale" under the previous text)[12]. The definition of "processor" under the CPA is similar to the definition of "service provider" in the CPRA. While the CPA offers a right to opt out of "targeted advertising" in addition to the opt out of sale, that right only applies to targeted based on online activity; moreover, there may be ambiguity as to which of the two opt-out rights a consumer is taking advantage of. The Attorney General should issue clarifying regulations to the terms "sale" and "processor" to forestall companies from engaging in unwanted data sharing even after a consumer attempts to exercise their opt-out rights.

C. User choice

Section 6-1-1313(2)(c) of the CPA mandates that UOOMS should "clearly represent[] the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data." As such, under Colorado law, an opt-out signal sent by a general purpose user agent by default and not at the direction of the user should not be construed as a legally binding opt-out choice.

However, a consumer's selection of a user agent that is promoted as protecting privacy should in many cases be interpreted as that consumer's choice to opt out of cross-context targeted advertising and the sale of their personal information. Certainly, when a consumer has installed a sole purpose browser extension to send an UOOM signal, such as GPC Privacy Choice,[13] the extension should not be required to obtain separate consent after installation to send a legally binding opt-out signal; that would introduce unnecessary friction and confusion into what is designed to be a simple option for consumers to exercise universal choices. Similarly, the choice to install a web extension that is specifically dedicated to limiting tracking and targeted

---

[11] Interactive Advertising Bureau, *IAB CCPA Compliance Framework for Publishers & Technology Companies*, https://www.iab.com/guidelines/ccpa-framework/

[12] Rachel Miller, *What Constitutes A Sale Under CCPA? Now That We know, There's No More Plausible Deniability?*, Ad Exchanger, (Oct. 21, 2021), https://www.adexchanger.com/data-driven-thinking/what-constitutes-a-sale-under-ccpa-now-that-we-know-theres-no-more-plausible-deniability/.

[13] GPC Privacy Choice, Chrome Web Store, https://chrome.google.com/webstore/detail/gpc-privacy-choice/ambkmcacbikgdchhjohhkfngeahpolnk.

advertising (such as Disconnect[14] or EFF's Privacy Badger[15]) should be interpreted as a user expressing a free choice to opt out of targeted advertising and the sale of their information. The same goes for selecting a *browser* that is promoted as stopping unwanted tracking and ad targeted (such as DuckDuckGo[16] or Brave[17]) — the choice of such a browser should be enough to evince an intent to stop tracking. As stated above, the CPA contains no provision or inference that a user must specifically invoke Colorado law or language to take advantage of the CPA's legal rights.

In cases such as these, the default for consumers would be using a general purpose user agent — choosing a privacy-focused user agent is a deliberate choice that should meet the CPA's requirements for exercising an UOOM. At some point, a user agent's tangential promotion of its privacy features may be too tenuous to infer an intent to stop tracking or targeted ads. However, given widespread consumer attitudes about cross-site tracking, the Attorney General should generally presume that a user's choice of a privacy-focused user agent evinces a choice to stop tracking and targeted ads. Supporting an expansive view would be consistent with the rulemaking principle of "promote consumer rights" — as well as interoperability with California's privacy opt-out rights that are roughly consistent with but slightly different from the CPA's articulation, and which do not impose burdensome design mandates for obtaining consent to opt out.

---

[14] Disconnect, https://disconnect.me/, promoting Disconnect as:

> We power privacy for over 750 million users.
> Block trackers in websites, apps, and email.
> Defend yourself from hyper-targeted attacks.
> Stop surveillance of your online activity.
> Prevent location and identity tracking.
> Take back control of your privacy and safety.

[15] Privacy Badger, https://privacybadger.org/#What-is-Privacy-Badger, promoting Privacy Badger as What is:

> a browser extension that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser, it's like you suddenly disappeared.

[16] DuckDuckGo, https://duckduckgo.com/, promoting the as "Privacy Browser App
Our private browser for mobile comes equipped with our search engine, tracker blocker, encryption enforcer, and more."

[17] Brave, https://brave.com/, promoting the Brave browser as "Stop being followed online: By default, Brave blocks the trackers & creepy ads on every website you visit. And that thing where ads follow you across the Web? We block that, too."

D. Re-opt-in

Despite the use of an UOOM, 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 UOOMs were created under Colorado law.

In practice, a provision allowing for consumer re-opt-in will primarily empower companies to pester users into granting permission to ignore the UOOM. 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.[18]

If the functional result of using an UOOM is simply that every site or app will then harass you for permission to ignore, the controls will end up being ineffective failures for Colorado consumers. For this reason, there is a strong policy argument to *prohibit* re-opt-in to ignore UOOMs under the CPA 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, though such a prohibition. However, such a blanket prohibition is likely disallowed by § 6-1-1306(1)(a)(IV)(C).

At the very least, the CPA 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).

In the event that a newly invoked UOOM setting contradicts an earlier permission to engage in targeted advertising or data sales, the newer UOOM setting should control. At this point, a company may ask for consent to engage in targeted advertising or data sale notwithstanding the general preference articulated by the UOOM. If the user's consent is consistent with the CPA's strict requirements, then it may be reasonable to allow the company to

[18] 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/.

prospectively disregard the general UOOM setting unless and until they revoke the specific exception granted to the company.[19]

Given the significant potential for abuse, companies should be required to respond to UOOMs with a prominent and persistent notice about the user's opt-out or re-opt-in state — as is required in regulations proposed by the California Privacy Protection Agency.[20] 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 Attorney General's regulations could provide that consumers should be able to assume that UOOM controls are operative, and only companies that disregard an UOOM control — either because the company believes it has re-opt-in consent or because it does not believe the signal conforms to the CPA's requirements for an UOOM — must provide prominent notice to consumers that the UOOM is not considered operative. This approach would incentivize companies to respect UOOM signals and disincentivize bad faith efforts to generate spurious consent. For either of these approaches, a company providing notice that an UOOM signal is being disregarded should include clear instructions on how to remedy a defective setting or how to revoke consent if the consumer so desires.

E. *Authenticating residency*

Section 6-1-1313(2)(f) of the CPA states that the Attorney General shall promulgate rules for UOOMs that:

> permit the controller to accurately authenticate the consumer as a resident of this state and determine that the mechanism represents a legitimate request to opt out the processing personal data for purposes of targeted advertising or the same of personal data pursuant to Section 6-1-1306(1)(a)(I)(A) or (1)(a)(I)(B).

The Attorney General should state that estimating residency based on IP address is generally sufficient for determining residency for purposes of the CPA, unless the company has a good faith basis to determine that a particular device is not associated with a Colorado resident. Companies already use IP-based geolocation in determining which privacy laws to comply with today, including large privacy compliance middleware companies that help other businesses implement compliance rules for their sites.[21] Absent a specific and justified doubt about a

---

[19] Such an approach would be consistent with what has been proposed under California law by the CPPA. *See* California Privacy Protection Commission, Text of Proposed Regulations, (Jul. 8, 2022), https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf, [Proposed CPRA Regulations], § 7025(c)(3).

[20] *See* Proposed CPRA Regulations, § 7025(c)(6).

[21] *E.g.*, Press Release, *OneTrust Cookie Consent Upgraded with Recent ICO, CNIL and Country- and State-Specific Guidance Built-in*, (Aug. 15, 2019), OneTrust, https://www.onetrust.com/news/onetrust-updates-cookie-consent-ico-cnil/.

particular consumer or device, companies should not be allowed to demand additional documentation or information from consumers before complying with UOOM requests. UOOMs are designed to be frictionless opt-out expressions for consumers; allowing every site or app to interrupt the browsing experience with a request for additional documentation would be contrary to the law's intent to protect user privacy and the regulatory principle of "promot[ing] consumer rights." It would also be inconsistent with California's recognition of UOOMs which does not allow for companies to mandate additional information before processing an opt-out request.[22]

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.[23] 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.[24] Consumer Reports research has also identified numerous dark patterns, including in smart TVs, food delivery apps, and social media.[25] 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.[26] 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.[27]

---

[22] Cal. Civ. Code § 1798.135(c)(1); Proposed CPRA Regulations §7025(c)(2).

[23] *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.

[24] 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/.

[25] *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/.

[26] *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/.

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

A. Requirements for consent

We recommend the Attorney General mandate the following requirements to ensure that company requests to disregard UOOMs or to process sensitive data for secondary purposes are valid and fair:[28]

- *Dedicated prompt*: Any consent for processing should be made pursuant to a dedicated prompt, separate from any privacy policy, license agreement, or other longform contract, that clearly and prominently describes the processing for which the company seeks to obtain consent.[29]
- *Symmetry of choice*: It should be at least as easy to decline consent for processing as it is to agree to such processing.[30]
- *Limitations on repeated requests for consent*: If a consumer declines consent for processing, the company should be prohibited from asking again for a specified period of time (such as six months).
- *Prohibition on abusive interfaces*: User interfaces and consent dialogs that subvert consumer free will and that utilize manipulative design or choice architecture should be prohibited.[31]
- *Conspicuous notice of opt-out/re-opt-in state*: As described, *supra*, § I.D, company should be required to provide clear notice if they are disregarding a user's UOOM because they believe that they have received consent to do so or because they dispute the legitimacy of the UOOM.[32]

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 Attorney General should develop a model interface — or

---

[28] The Attorney General's requirements for consent for processing sensitive data *in direct service of fulfilling a consumer request* could potentially be less stringent. In many cases, such processing which is necessary to deliver a good or service requested by the consumer, is likely to be contextually expected and uncontroversial — in such cases, it may be reasonable to infer consent by the consumer's request of the good or service itself.

[29] *See* Amendment in the Nature of a Substitute, revised text of the "American Data Privacy and Protection Act" as passed by the House Energy and Commerce Committee, (Jul. 20, 2022), https://cdt.org/wp-content/uploads/2022/07/AINS-ADPPA-07192022.pdf, ["ADPPA"], § 2(1)(B)(i), Proposed CPRA Regulations, § 7004(a)(1).

[30] *See* ADPPA, § 2(1)(B)(vi); Proposed CPRA Regulations, § 7004(a)(2).

[31] *See* ADPPA, § 2(1)(D); Proposed CPRA Regulations, § 7004(a)(3)-(4).

[32] *See* Proposed CPRA Regulations, § 7025(c)(3).

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 Attorney General 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. If over time the Attorney General's exemplary guidance proves insufficient to rein in the use of dark pattern interfaces that subvert consumer intent, the Attorney General must be more prescriptive and provide a narrower range of choices and specific language for companies that purport to obtain consent for data processing.

B. Non-retaliation

One bedrock principle of privacy law is that companies shouldn't punish consumers for making privacy choices. Privacy should be recognized as an inalienable and fundamental right, not merely an asset to be bartered away. Charging consumers for privacy would also have a disparate impact on the economically disadvantaged and members of protected classes who may not be able to afford the luxury of paying for fundamental privacy rights.

Section 6-1-1308(1)(c)(II) provides "A controller shall not . . . based solely on the exercise of a right and unrelated to feasibility or the value of a service, increase the cost of, or decrease the availability of, the product or service." This non-retaliation language is the strongest among the state privacy laws in the country, stronger than similar language contained in the CPRA which explicitly allows differential treatment based on the value of a consumer's data.

The Attorney General should clarify in this rulemaking proceeding that any differential treatment or pricing based on a consumer's choosing to exercise a privacy choice is prohibited by the CPA. This should include not just when consumers exercise access or deletion rights or opt out of sharing or targeted advertising, *but also when they refuse consent for functionally unnecessary data processing*. For example, Google should not be able to condition use of its Gmail service on a consumer's agreeing to let Google track them around the web and in other mobile applications. The Attorney General should make clear that such a mandate runs counter to the text and purpose of the CPA and does not constitute valid consent.

Relatedly, the Attorney General should clarify § 6-1-1308(1)(d) of the CPA which makes an exception to the law's non-retaliation provisions for a "consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount, or club card program." The term "bona fide" is not defined within the text of the statute and as such potentially subject to abuse by bad actors seeking a general loophole to the non-retaliation principle. Companies should not be able to impose differential treatment simply by labeling any conduct as a "bona fide" loyalty or discount program. Consumer Reports has no objection to data processing necessary to maintain loyalty programs, so long as the data is simply used to track engagement for loyalty rewards.

However, the Attorney General's regulations should specify that data cannot be shared or sold to third parties to monetize data for unrelated purposes as part of a "bona fide" rewards program.

III. PROFILING AND "LEGAL OR SIMILARLY SIGNIFICANT EFFECTS"

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. Also, some companies claim that correlations between unrelated data can predict behavior or other outcomes, with little evidence, often leading to discriminatory results.[33]

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, but we can put guardrails in place through policy that can mitigate or prevent harmful effects of discrimination.

Fundamentally, reaching consensus on a definition for "profiling" is an important step to properly regulating algorithms for specific sensitive applications. We ask the Attorney General to clarify exactly what kinds of statistical methods and in what context or application this bill is intended for. The current definition is overbroad and could encompass simple statistical methods and applications that could be rather inconsequential for Coloradans. "Profiling" is defined as "any form of automated processing" for particular applications. However, automated processing could refer to a number of different statistical methods that range from simple mathematical formulas to complicated algorithms such as neural networks that companies claim can make predictions or classifications about individuals. For example, consider an HR department within a company using algorithms to parse resumes for an open job position. Using a simple computing tool that can identify the number of years an individual has worked based on their college graduation date obtained from their resume is much different from using a neural network to "holistically" look at a resume and determine whether someone is qualified for a job (the former is a more objective and straightforward process than the latter).

---

[33] Arvind Narayanan, Princeton University, *How To Recognize AI Snake Oil,* https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf.

A. Transparency

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 occuring at all. There are virtually no laws 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 decisionmaking involving significant legal effects, consumers deserve transparency. We advise that for algorithms with significant legal effects (including housing, credit/lending, insurance, employment, criminal justice), meaningful transparency measures are needed in order to identify and mitigate discrimination.

Companies often use multiple data points that are fed into the algorithm to make a decision about how a consumer behaves. Companies should thus disclose what types of data they collect, the specific data that the company 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). 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 such as race, gender, and religion are prohibited. 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."[34] 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 information that must be corrected in a timely manner (or be provided a clear explanation as to why the data is not inaccurate).

---

[34] *Why am I seeing ads from an advertiser on Facebook?*, Facebook, https://www.facebook.com/help/794535777607370.

B. Banning pseudoscience and other harmful technology

There are certain harmful applications of AI where improved transparency and better consumer control of data are not enough. 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.[35] 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.[36] Generally, using AI to predict subjective processes like job success and recidivism is likely to 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 previously marginalized. While unfair and deceptive practices are outlawed at the state and federal levels, the Attorney General needs to make more clear what kinds of AI applications fall under this category.

C. Opting out and prohibitions

For automated decisionmaking applications with significant legal effects, sometimes simply notifying the consumer that they are being profiled is not enough. Providing a consumer with the option to opt out of this type of profiling places an excessive burden on the consumer, but also does not address the fact that these algorithms, which can often be inaccurate or discriminatory, provide few ways for a consumer to contest a potentially wrong decision if they choose to not opt out. While the intention of many companies using complex algorithms is to attempt to provide more fair decisions, the technology is simply not at a place where it is accurate or explainable enough for it to be used safely. Consumers' civil rights are too important, and we should not normalize the use of unexplainable algorithms in these contexts.

More complicated algorithms like neural networks, that are more commonly used in automated decisionmaking, are often difficult to explain how they arrive at their decisions due to their opaque "black box" nature. In the cases of applications with significant legal effects, consumers deserve real and meaningful explanations as to how decisions are made about them, particularly when they affect someone's access to life opportunities or even their liberty. For this

---

[35] Arvind Narayanan, Princeton University, *How To Recognize AI Snake Oil,* https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf.

[36] Drew Harwell, *Rights group files federal complaint against AI-hiring firm HireVue, citing 'unfair and deceptive' practices,* The Washington 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/.

reason, the Consumer Financial Protection Bureau recently clarified that if a creditor is using a complicated algorithm that denies credit to an applicant and the creditor cannot explain why the algorithm arrived at its decision, then it should not be used.[37] This clarification sets an important precedent — if a company is using algorithms that are complicated enough that they are not able to explain how it arrives at its conclusions, then it should not be used for applications with significant legal effects. With these sensitive applications, consumers deserve the ability to contest false or inaccurate decisions, something they are not able to do if the algorithms making decisions about them cannot be properly explained.

IV. OFFLINE AND OFFWEB

The CPA does not make a distinction between information collected online or offline — all information "that is linked or reasonably linkable to an identified or identifiable individual" is covered.[38] All of the CPA's rights apply to this information, including the rights to access, correct, delete, port, and to opt out of data sales and targeted advertising.[39]

While there have been several efforts to develop UOOMs that apply to online data sharing, there has been less attention paid to equivalent offline UOOM mechanisms. While some online UOOMs are already sufficiently robust to be recognized as conveying binding opt-out requests, the Attorney General should explore and invite comment on approaches to implement offline approaches. One potential solution would be for the Attorney General 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 Attorney General 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,

---

[37] *Adverse action notification requirements in connection with credit decisions based on complex algorithms*, Consumer Financial Protection Bureau (May 26, 2022), https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.

[38] *See* § 6-1-1303(17).

[39] While "targeted advertising" is defined as targeted based on online activity, the right to not receive ads targeted based on online activity applies offline as well. So a Colorado resident has the right to opt out of receiving, for example, direct mail based on their online activity. *See* § 6-1-1303(25).

indicating that this is an easy way for consumers to opt out of telemarketing messages.[40] 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.

In many cases, online UOOM opt-outs should apply to offline targeted advertising and data sales as well. Companies that receive an online request to opt out of either targeted advertising or data sales should propagate that opt-out to other contexts as well if the user is authenticated to the service by an identifier that applies in other contexts. However, companies should not be required to collect additional personal information or authenticate users just to process opt-outs. If a company only tracks a user by a pseudonymous identifier online, it should not be mandated to collect additional information to process the opt-out — instead, the opt-out may only apply in that case to one browser or operating systems. On the other hand, the company could offer to let the user login to an account to allow the opt-out to apply to the user's account in all settings.[41]

For example, if a user is logged into the New York Times online and transmits a request to opt out of data sales and targeting advertising — either through an individual opt-out or an UOOM — the New York Times should apply that opt-out across the user's account. The New York Times should honor that opt-out request when the user logs in on other browsers or into the New York Times mobile application. It should also honor the opt-out request as it applies to offline data sharing and sales. On the other hand, if the user has not logged in and is only identifiable by a cookie, the New York Times need only apply the opt-out to that particular browser, and should not be allowed to require the user to log in to honor the request. It may at its own discretion prompt the user to login if the user wants the opt-out to apply account-wide.

****

We thank the Attorney General's office 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.

---

[40] 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.

[41] *See* Proposed CPRA Regulations, § 7025(c)(2).