Initial Comments of Consumer Reports
In Response to the
Colorado Department of Law's
Proposed Draft Rules
Interpreting the Colorado Privacy Act

by

Justin Brookman, Director of Technology Policy

November 7, 2022

Consumer Reports[1] appreciates the opportunity to provide initial comments on the proposed rules (Draft Rules) issued by the Colorado Department of Law interpreting the Colorado Privacy Act (CPA). We thank the Department of Law for their diligent and timely work in publishing the Draft Rules and for soliciting input to make the CPA most effective for consumers. Consumer Reports had previously submitted comments this summer to the Department of Law in response to its initial pre-draft solicitation of feedback.[2]

We are submitting these initial comments on the Draft Rules by November 7th in order to inform the stakeholder meetings taking place starting November 10th. Consumer Reports has registered to speak at the first session on "Consumer Rights and Universal Opt-Out Mechanisms." We will be focusing our oral comments on two issues: Universal Opt-Out Mechanisms (UOOMs) and bona fide loyalty programs. Those two topics are the focus of this initial set of comments. We will submit more detailed comments on the full set of Draft Rules in early 2023.

Consumer Reports is also a founding member of the Global Privacy Control (GPC) project, an open-source, web-based UOOM with over 50 million unique users each month.[3] Consumer Reports's Director of Technology Policy Justin Brookman is a contributing editor to the project. However, these comments reflect the views only of Consumer Reports and are not necessarily representative of other project participants.

Consumer Reports is supportive of most of the Draft Rules issued by the Department of Law. We recommend a number of narrow modifications on a few key points to ensure that the CPA's new rights are functionally usable and effective for consumers. Specifically, we urge the Department of Law to:

- Issue clearer guidance on how companies may authenticate residency and legitimacy
- Provide less prescriptive, Colorado-specific mandates on UOOM interfaces

---

[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] Justin Brookman and Nandita Sampath, 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, Consumer Reports, (Aug. 5, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/08/Colorado-rulemaking-input-summer-2022.pdf.

[3] Global Privacy Control, https://globalprivacycontrol.org/..

- Expand exception for privacy-focused user agents sending UOOM signals to preinstalled applications
- Specify that Controllers should propagate opt-out requests from authenticated consumers to other contexts
- Remove ambiguities around requirements that UOOMs not "unfairly disadvantage" other Controllers or engage in "self-dealing"
- Remove mandates that UOOMs be an "open system or standard"
- Make notice of opt-out/re-opt-in state mandatory
- Tighten the definition and interpretation of bona fide loyalty program to eliminate loopholes

We will explain each of these points further below in discussing various sections of the proposed Draft Rules.

Section 5.02 Rights Exercised

Section 5.02(C) provides:

> A Universal Opt-Out Mechanism may express a Consumer's choice to opt out of the Processing of Personal Data for all purposes subject to the opt-out right or it may express a Consumer's choice to opt out of the Processing of Personal Data for one specific purpose only. A Universal Opt-Out Mechanism may offer "all purposes" or "specific purposes" options, or both.

We disagree that UOOMs should be required to clearly present to users the option to opt out of "all purposes," "specific purposes," or both. UOOMs are likely to be general, cross-jurisdiction tools which may have the effect of exercising different rights in different states (or countries). In California, a UOOM may opt a user out of "sharing," in Germany, it may opt a user out of data used for "legitimate interests,"[4] and in Colorado it may opt a user out of "targeted advertising" and "sale of data." Even in Colorado alone, the rights to opt out of "targeted advertising" and "sale" 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, the Draft Rules should be revised to clarify that, 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 jurisdictions that offer consumers

[4] Robin Berjon, *Do not sell my European data: GPC under the GDPR*, Robin Berjon, (Jul. 16, 2021), https://berjon.com/gpc-under-the-gdpr/.

slightly different formulations of legal rights. Colorado should not require UOOMs to specifically invoke each Colorado right; otherwise, UOOMs would in practice have to articulate a sprawling boilerplate of all possible rights to be invoked around the world. Instead a UOOM should reasonably be interpreted as exercising the rights associated with the behaviors intended to be addressed by the UOOM. The Department of Law should make that assessment when considering UOOMs for inclusion in its public registry.

Section 5.03 Notice and Choice

We recommend removing § 5.03 of the Draft Rules, or at least removing §§ 5.03(A)(2) and 5.03(A)(3). These provisions mandate extensive and potentially ambiguous disclosures from UOOM providers that a consumer is unlikely to understand or engage with in practice. Section 5.03(A)(2) requires UOOM providers to "[if] applicable, state that the Universal Opt-Out Mechanism has been recognized by the Colorado Attorney General." Section 5.03(A)(3) would be even more difficult for UOOM providers to comply with: it requires UOOM providers to "clearly describe the mechanisms's limitations," including which specific rights are to be invoked and whether the signal will have a legal effect in other contexts, such as on mobile devices.

UOOM providers who do not otherwise have significant legal compliance obligations (such as the developer of a browser extension) may not have the capacity to keep up to date with how UOOM signals are interpreted in 50 different states and hundreds of countries around the world. Requiring UOOM providers to maintain a list of the specific legal implications of receiving the UOOM signal in all these varying jurisdictions is burdensome enough; presenting such notice to consumers would be overwhelming. Moreover, the legal limitations of the UOOM described in § 5.03(A)(3) may not even be clear to the most sophisticated UOOM developer. Even under these Draft Rules, it is not entirely clear when a consumer's opt-out choice through a browser would subsequently be binding on a Controller who engages with the consumer through a mobile application or offline. Finally, it is not entirely where and how these disclosures should be presented to consumers. Section 5.03(A)(4) states that UOOM developers must not use "dark patterns" in making these disclosures to consumers. If in practice that means consumers must click through several standalone statements about the UOOM's various legal effects and limitations, that would be likely to confuse and frustrate consumers and limit adoption.

Relatedly, it is unclear how such disclosures should be made retroactively. Today, over 50 million users are transmitting GPC signals to websites through their browsers. The user agents sending these signals should not have an obligation to push notice of a change in legal status each time a jurisdiction revises a statute or issues a new interpretation affecting the legal implications of UOOM signals. Notably, California and Connecticut — the other states that explicitly provide for opting out through UOOMs — do not mandate such notice requirements.

Instead, Colorado's rules should be flexible. UOOMs such as GPC are general purpose, not state- or jurisdiction-specific — they are designed to express a preference to limit data processing which will necessarily have different legal effects in different jurisdictions. For Colorado consumers, the state of Colorado should provide the definitive guidance as to what the legal consequences are for which privacy signals. As such, § 5.03(A) should also be revised as we have suggested to revise § 5.02(C) above to eliminate any implication that the UOOM user interface must call out Colorado-specific rights when activated by a consumer.

Finally, we recommend renaming § 5.03 if not deleting it altogether. The notion of "notice and choice" has become widely discredited in privacy circles in recent years;[5] it is associated with the conceit that consumers read the lengthy and evasive disclosure in website privacy policies and knowingly consent to the conditions described therein by continuing to browse that service. Indeed, the choice of this term is arguably indicative of the problems with the requirements in §§ 5.03(A)2-3 — mandating consumers be presented with detailed disclosures they did not ask for and are unlikely to read in detail. The term "notice and choice" does not appear in the text of the Colorado Privacy Act. As such, we would recommend either deleting this section entirely or changing the name of this section to Disclosures to Consumers or something similar.

Section 5.04 Default Settings

In general, we are supportive of the basic framework laid out in § 5.04: general purposes user agents may not send UOOM signals by default, but user agents specifically marketed as designed to safeguard privacy may reasonably infer a consumer's intent to broadcast a UOOM signal without further user interaction. Mandating additional consumer dialogues after a user has made the choice of a privacy-focused user agent would introduce unnecessary friction and confusion into what is designed to be a simple option for consumers to exercise universal choices. In general, the framework laid out in § 5.04 seems like a fair compromise that is not overly prescriptive and accords with a reasonable interpretation of user intent.

However, we would disagree with the Draft Rules' provision that a consumer's use of a *preinstalled* privacy-focused user agent would not constitute "affirmative, freely given, and unambiguous choice" to stop data sales or targeted advertising. For example, a mobile phone or laptop could preinstall several different browsers from which a consumer selects in order to access the web. A consumer's choice of a privacy-focused one such as DuckDuckGo should be interpreted as an affirmative choice to stop unwanted tracking just as much as the user's installation of the same browser would be. Similarly, a user could choose to purchase a

[5] *E.g.*, Cameron F. Kerry, *Why protecting privacy is a losing game today—and how to change the game*, Brookings, (Jul. 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

privacy-focused device that uses privacy-focused apps as default options (such as ProtonMail and Brave). In that case, the choice of the phone and use of those apps would be sufficient evidence of intent to protect their information.

The text of the CPA offers no rationale for distinguishing between apps that are preinstalled or not. We urge the Department of Law to simplify the Draft Rule and provide that the use of *any* privacy-focused user agent would be reasonably interpreted as evincing an intent to invoke legal privacy rights. This revision 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 similar limitations on preinstalled apps before sending UOOM signals.

Section 5.05 Personal Data Use Limitations

We generally support the provisions contained in this section, including the prohibition on secondary use and secondary data collection. To further clarify these requirements, we recommend including a new example in § 5.05(A) stating that the fact that a particular device sends an UOOM signal may not be used for digital fingerprinting purposes to more definitively identify that device in other contexts.

We also support the provision in § 5.05(C) that a Controller may ask a consumer for additional information in order to apply the requested opt-out in other contexts. However, in the event that the user is *already* authenticated to the Controller, the Rules should be clear that Controller should automatically and by default apply the requested opt-out rights to other contexts, such as on other devices when the consumer is authenticated, as well as offline use of that consumer's data.

Finally, we urge the Department of Law to provide greater clarification on what data is strictly necessary to confirm a user is a resident of Colorado and that the mechanism represents a "legitimate" request to opt out of certain data processing. In Consumer Reports's investigation into the usability of new privacy rights in California, we found examples of companies requiring consumers to fax in copies of their drivers' license in order to verify residency and applicability of CCPA rights.[6] If every site in Colorado responded to a UOOM signal with such a request, in practice UOOMs would be practically unusable and ineffective.

[6] 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.

As a better alternative, many companies comply with state privacy laws by approximating geolocation based on IP address.[7] The Department of Law should revise the Draft Rules to clearly state that estimating residency based on IP address is generally sufficient for determining residency and legitimacy 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 or is otherwise illegitimate. The Rules should further state that additional data processing to confirm residency or legitimacy absent specific evidence to the contrary is prohibited.

Section 5.06 Technical Specification

We generally support the provisions in § 5.06. As discussed above, however, we would request that the Department of Law provide clearer guidance on assumptions and what processing is appropriate to determine when a consumer is a resident of the state of Colorado and when an opt-out request is "legitimate." The Department of Law should clarify that if the IP address is one generally associated with Colorado residents and there are no special circumstances indicating misbehavior, the Controller should presume that the user is a resident of the state of Colorado and that the opt-out request is legitimate.

We also urge greater clarity on 5.06(F)'s admonition that a UOOM developer cannot "unfairly disadvantage" any Controller. The example provided that UOOMs "may not treat different Controllers differently" is confusing and arguably at odd with language in § 5.06(C)(2)'s indicating that a UOOM should allow a consumer "to opt out of one or more Controllers that recognize the mechanism, to opt out of one or more domain, or to opt out of Processing by all Controllers that recognize the mechanism."

In fact, UOOMs should be allowed to treat different Controllers differently. A consumer may want to install a UOOM that is targeted specifically at data brokers (or may configure a general purpose UOOM to only target data brokers); in that case, a consumer should be empowered to only send opt-out requests to data brokers. A UOOM may also process re-opt-in exceptions on behalf of the user, keeping track of the companies that a user grants an exception to to their general preference not to have used for certain processing. In that case, the UOOM may not send an opt-out signal to those companies to which the consumer has granted an exception.

Similarly, it is not clear what "self-dealing" is prohibited by § 5.06(F) of the Draft Rules. If that provision merely prohibits a UOOM developer from transmitting opt-out signals to every Controller except itself, such a rule may be defensible, though one could envision a scenario where a user wants to have one privacy-preserving service deliver targeted ads while blocking all

[7] *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/.

other tracking. In any event, more clarity as to what constitutes prohibited "self-dealing" would be helpful.

Section 5.07 System for Recognizing Universal Opt-Out Mechanisms

In our initial comments to the Department of Law on this privacy rulemaking, Consumer Reports strongly encouraged the development of a definitive list of UOOMs that Controllers must adhere to. We were pleased to see the Draft Rules include such a provision, and believe that the registry system described in § 5.07(A) will provide needed clarity and certainty for consumers, Controllers, and UOOM developers.

We support the systems requirements for UOOMs described in §§ 507(C)(1) and (3). However, we do not believe that § 507(C)(2)'s mandate that a UOOM be an "open system or standard" and available to others for free or on "fair, reasonable, and non-discriminatory terms" is necessary or helpful. While UOOMs like the GPC are open-source and open to use by others, other UOOMs, for closed systems for example, may not necessarily comply with § 507(C)(2)'s requirements. Until recently, Apple had a universal "Limit Ad Tracking" setting available for iOS devices that allowed users to set a general preference to stop tracking for all installed apps. Similarly, the developer of a Smart TV ecosystem could develop a system-wide global signal to allow users to exercise opt-out rights to Smart TV apps. UOOMs designed for the open web may not be directly transferable to such environments. While we support and encourage the development of open standards, the Draft Rules' mandate for openness is not supported by the text of the Colorado Privacy Act and may deter the development and deployment of useful tools for consumers to globally exercise rights on certain platforms. If nothing else, these considerations should be moved to § 507(D) instead as factors for the Colorado Department of Law's office to weigh in deciding whether to add certain signals to the UOOM registry.

Section 5.08 Obligations on Controllers

Section 508(D) provides:

> Unless a Controller is Authenticating a Consumer as permitted by C.R.S. § 6-1-1313(2)(f), a Controller may not require a Consumer to login or otherwise Authenticate themself as a condition of recognizing the Consumer's use of the Universal Opt-Out Mechanism.

We strongly object to 508(D)'s implication that Controllers may mandate that users log onto accounts in order to authenticate Colorado residency or that an opt-out request is legitimate. Allowing Controllers to disregard UOOMs unless consumers authenticate their identity to the Controller would make UOOMs practically useless for consumers — instead, every site could

interrupt the user experience with an interstitial asking the user to log on or create an account in order to effectuate the opt-out. This guidance is also at odds with § 5.05(C) of the Draft Rules that says a site may *optionally* ask for additional information from the user in order to apply opt-out rights to other contexts.

Importantly, the CPA states that a Controller may authenticate the *residency* of the user sending a UOOM — not the *identity*. As requested earlier, we urge the Department of Law to state that associating a user with a Colorado-based IP address is sufficient authentication of residency under the law, and further data processing for residency authentication and legitimacy is prohibited absent some special evidence of wrongdoing.

We previously recommended revising § 5.05(C) to clarify that if a user is presently authenticated to the Controller, then the Controller should frictionlessly apply the user's opt-out requests to other uses of that consumer's identifiers or when that user is authenticated on other devices. We recommend clarifying that principle in § 5.08(A)(2) as well to state that once a Controller receives a UOOM request when a user is authenticated, then the Controller should continue to treat that user as opted out across other contexts as well unless and until the user specifically overrides the opt-out.

We also previously suggested revising §§ 5.02(C) and 5.03(A) to clarify that cross-jurisdiction UOOMs need not call out in the user interface Colorado specific rights to the user. Relatedly, we recommend revision § 5.08(A)(2) to remove the phrase "as indicated by the mechanism," which implies that the UOOM must invoke specific Colorado legislative text in order to be operational.

We support the text of §§ 5.08(B) and (C).

Section 5.08(E) of the Draft Rules states that companies "may" indicate compliance with an opt-out preference signal. This permissive phrasing is not appropriate for a rulemaking; presumably Controllers "may" engage in all sorts of behaviors not otherwise proscribed by the Draft Rules. By making such disclosure optional, it is likely that few if any companies will in fact offer such transparency to users as to whether their opt-out choices are effective or not. We recommend revising this language to mandate conspicuous notice about opt-out/re-opt-in state, as is required under California's draft CPRA regulations.

Alternatively, as we suggested in our initial comments to the Department of Law, the regulations could provide that consumers should be able to assume that UOOM controls are operative, and only companies that *disregard the UOOM* — 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 alternative approach would incentivize companies to respect UOOM signals and disincentivize bad faith efforts to generate spurious signals. 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.

Section 5.09 Consent after Universal Opt-Out

Consumer Reports is generally supportive of the language in this section, but will provide more detailed feedback on related sections on consumer consent at a later date.

Section 6.05 Bona Fide Loyalty Programs

We are concerned that the Draft Rules interpreting the CPA's exception for "bona fide loyalty programs" are too vague and could offer companies wide loopholes to deny consumer rights by simply labeling any data sale or targeted advertising practice a "bona fide loyalty program." We urge the Department of Law to adopt a more precise definition and to provide clearer examples of prohibited behavior that does not fall under this exception.

Sections 6.05(B) and (C) reasonably provide that if a consumer deletes or does not provide consent for the processing of certain data that is functionally necessary to operate a loyalty program, then the consumer cannot expect to enjoy the benefits of the loyalty program. We have no objection to these provisions — if a consumer insists on deleting a record of previous purchases and loyalty points, they cannot expect to later be able claim loyalty rewards based on that data. However, if a consumer deletes or does not agree to the collection of data that is not functionally necessary to track loyalty behavior, then the Controller should be prohibited from differential treatment even under the guise of the loyalty program.

Similarly, § 6.05 should clarify that exercising opt-out rights related to data sales or targeted advertising should never (or almost never[8]) interfere with the operation of a bona fide loyalty program. Controllers do not need to sell data to others or to engage in cross-site targeted advertising in order to operate a bona fide loyalty program — such behaviors have nothing to do with the tracking of purchases to offer discounts or first-party advertising. As such, Controllers should be prohibited from denying service to or giving differential treatment to consumers who exercise such opt-out rights under the guise of operating loyalty programs.

[8] Depending on the Department of Law's interpretation of the term "sale," certain joint loyalty programs that allow consumers to spend loyalty rewards on other brands (such as an airline loyalty program that allows conversion of accrued miles to a partner hotel chain's point programs) could be impacted on a blanket prohibition on data "sales" conducted pursuant to a loyalty program. We would support an accommodation that allows consumers to engage in joint loyalty programs or programs that allow transfer of loyalty rewards to other merchants.

Worryingly, § 7.05 (Consent After Opt-Out) implies that Controllers may in fact be able to do just that:

> If a Consumer has opted-out of the Processing of Personal Data for the Opt-Out Purposes, and then initiates a transaction or attempts to use a product or service inconsistent with the request to opt-out, *such as signing up for a Bona Fide Loyalty Program that also involves the Sale of Personal Data*, the Controller may request the Consumer's Consent to Process the Consumer's Personal Data for that purpose, so long as the request for Consent complies with all provisions of 4 CCR 904-3, Rules 7.03 and 7.04. [emphasis added]

Section 6.05(E)(1)(c) also implies that consumers may be deprived of the full value of loyalty programs if they opt out of the sale of their data or the use of their data for targeted advertising. This interpretation of the CPA misunderstands how bona fide loyalty programs work and would fundamentally undo the CPA's otherwise strong nonretaliation language contained in § 6-1-1308(1)(c)(II) of the law. We recommend these sections be deleted, and the definitions of "bona fide loyalty program" and §§ 6.05 and 7.05 be revised to clarify that opt-out rights necessarily do not interfere with the operation of bona fide loyalty programs.

We also recommend including two new examples — such as the ones below — to clarify the interaction between opt-out rights and bona fide loyalty programs:

- An online gaming company gives consumers who opt out of the use of their data for targeted advertising access to fewer free games on the service. The company argues its behavior is justified because the data is part of a "loyalty program" that allows the company to monetize data and offer free service. The company's differential treatment is prohibited because sale of data is not necessary to operate a "bona fide loyalty program" that provides incentives to consumers for repeat business or engagement.
- An airline collects various data about its customer's behavior and sells some of this information to data brokers. The airlines also uses some of this same data to operate a loyalty program whereby a consumer may spend accrued points for discounted or free travel. If a consumer opts out of the sale of this data to data brokers, the airline is prohibited from limiting or disadvantaging the consumer's participation in the loyalty program, since the opt out of data sales has no effect on the airline's ability to track purchases and miles traveled.

****

Thank you very much again for the opportunity to provide feedback on the initial Draft Rules. As mentioned previously, we will be following up with additional recommendations on other sections of the Rules, including additional specific language suggestions for inclusion in the final version. We look forward to continuing to engage with the Department of Law on this important proceeding. 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.