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

by

Justin Brookman, Director of Technology Policy
Matt Schwartz, Policy Analyst

January 18, 2023

Consumer Reports[1] appreciates the opportunity to provide comments on the Revised Draft Rules (revised rules or rules) issued by the Colorado Department of Law (Department) interpreting the Colorado Privacy Act (CPA). We thank the Department for its diligent work to consider stakeholder feedback and for incorporating many of our suggestions into these revised rules, which make the CPA more effective for consumers in many ways. Consumer Reports had previously submitted comments upon the initial release of the draft rules in late 2022,[2] as well as in the summer when the Department of Law issued its pre-draft solicitation of feedback.[3]

We are submitting these comments on the Revised Draft Rules by January 18th in order for them to be considered as part of any additional revisions presented at the CPA rulemaking hearing on February 1, 2023. Consumer Reports has also registered to speak during the public forum on that same date.

We note the Department's particular interest in several questions relating to bona fide loyalty programs and the use of IP addresses for authentication, some of which we responded to in our previous round of comments. We include and expand upon our previous commentary on those and other topics here.

Consumer Reports is also a founding member of the Global Privacy Control (GPC) project, an open-source, web-based Universal Opt Out Mechanism (UOOM) with over 50 million unique users each month.[4] 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.

While Consumer Reports is supportive of some of the Revised Draft Rules issued by the Department of Law, we remain some concerned with some provisions that did not change in the revisions (particularly relating to UOOMs and bona fide loyalty programs), as well as with

---

[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, Initial Comments of Consumer Reports In Response to the Colorado Department of Law's Proposed Draft Rules Interpreting the Colorado Privacy Act, Consumer Reports, (November 7, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/11/CR-comments-on-initial-CPA-regs-Nov-2022-4.pdf

[3] 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.

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

several new changes that appear to have been made against the consumer interest. 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.

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

Rule 4.02 Submitting Requests to Exercise Personal Data Rights

Draft Rule 4.02(F) currently states:

If a Consumer or Authorized Agent submits a request for an Opt-Out Purpose in a manner that is not one of the Controller's specified Data Rights request methods, or the request is otherwise deficient in a manner unrelated to the Authentication process, the Controller shall either: (1) treat the request as if it had been submitted in accordance with the Controller's specified request methods, or (2) provide the Consumer with information on how to submit the request or remedy any deficiencies in the request.

We suggest a minor tweak so that a controller shall provide the consumer *or the authorized agent,* if the consumer has designated one to carry out the opt-out purpose, with the information on how to submit the request or remedy any deficiencies. Consumers who have designated an authorized agent to carry out their rights requests or opt-outs tend to do so in order to avoid extensive communication with controllers and expect the authorized agent to simplify the data management process. Allowing controllers to send remedial opt-out information to the consumer instead of the authorized agent would frustrate that process. In such cases, controllers should route the corrective information directly to the authorized agent, rather than the consumer who would then have to take the additional step of sending it to their authorized agent.

Rule 4.03 Right to Opt Out

Draft Rule 4.03(C) states that a controller shall comply with an authorized agent's opt-out request "so long as the Authorized Agent's request permits the Controller to Authenticate the identity of the Consumer and the Authorized Agent's authority to act on the Consumer's behalf." In order to prevent controllers from stifling opt-out requests by unfairly deeming authorized agents unauthorized to submit opt-out requests, we suggest that the Department of Law add to this subsection objective criteria whereby an agent can demonstrate proof of authority. For example, any authorized agent that can produce a certificate of good standing and signed authorization note from the consumer shall be deemed capable of sending an opt-out request. Alternatively, the Department of Law could consider maintaining a public list of authorized agents (or at least services that provide authorized agents) that have been recognized to meet the standards of the law. Any standards that the Department adopts to guide controller authentication of authorized agents in the context of opt-out should also apply to all data rights, as contemplated in Rule 4.08.

Relatedly, Rule 4.08(C) implies that a controller can request additional personal data to authenticate an authorized agent's authority if the controller cannot authenticate the authority using data it already maintains on a consumer. This construct misunderstands the nature of an authorized agent; controllers will not typically have personal information that can authenticate the authority of an authorized agent ahead of time, that information will most commonly be provided upon an authorized agent's rights request. The Department should adopt the revision suggested in the previous paragraph to establish objective criteria by which an agent can demonstrate proof of authority and then revise this section to read that a controller shall avoid requesting additional personal data from an authorized agent unless it cannot authorize its authority using the objective criteria.

Section 5.02 Rights Exercised

We continue to believe that Section 5.02(C) should be simplified. 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,"[5] 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.

The rules should be revised to clarify that, by default, UOOMs should be interpreted as invoking all opt-out 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 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 for Universal Opt-Out Mechanisms

We recommend removing Section 5.03 of the Draft Rules, or at least removing Section 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 any limitations that may be applicable to the mechanism,"

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

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 Section 5.03(A)(3) may not even be clear to the most sophisticated UOOM developer. Even under these Revised 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.

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, Section 5.03(A) should also be revised as we have suggested to revise Section 5.02(C) above to eliminate any implication that the UOOM user interface must call out Colorado-specific rights when activated by a consumer.

Section 5.04 Default Settings for Universal Opt-Out Mechanisms

We strongly disagree with the proposed revision to Section 5.04(B) eliminating language indicating that a consumer's selection of a privacy-protective tool is sufficient to infer an intent to stop tracking. As discussed above, UOOMs are typically general purpose and not jurisdiction-specific; requiring UOOMs to specifically invoke state-specific legalistic formulations about various and overlapping opt-out rights will lead to voluminous and confusing disclosures that in practice will make it more difficult for Colorado consumers to exercise their privacy rights. The Department of Law should revert to previous language indicating that selection of a privacy-focused user agent indicates an intent to stop tracking.

We also continue to disagree with the provision that states 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 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.

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. We appreciate the inclusion of our suggested revision to include a new example in Section 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 Section 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. For example, under the latest round of rules implementing the California Privacy Rights Act, covered businesses are required to treat opt-out preference signals as a valid request for any consumer profile, including pseudonymous profiles, associated with the browser or device that sent the signal.[6] Currently, the draft rules are ambiguous as to whether companies that receive UOOM requests through a browser are required to honor that opt out in other contexts.

Finally, as discussed in greater detail in later sections, 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.[7] If every site in Colorado responded to a UOOM signal with such a request, in practice UOOMs would be practically unusable and ineffective. In our view, associating a user with a Colorado-based IP address should be sufficient authentication of residency under the law.

Section 5.06 Technical Specification

---

[6] California Privacy Protection Agency - Modified Text of Proposed Regulations, Section 7025(c)(1), (Nov. 3, 2023), https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf

[7] 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-Prote cted_092020_vf.pdf

We are troubled by the deletion of Section 5.06(A)(2), which allowed UOOMs to maintain a "do not sell list" in lieu of sending an opt-out signal. Do not sell lists represent an important alternative to the UOOM signal in that they may lower the barrier to consumers expressing their privacy preferences, especially given the limitations placed on UOOM installations and defaults discussed above. For example, certain consumers may not be comfortable with downloading a browser plug-in or might not own devices with UOOM capabilities but nevertheless wish to assert their privacy rights. Ensuring that privacy protections flow equally to consumers regardless of tech savvy or privacy literacy should be an important goal of privacy legislation and regulation.

On the other hand, we appreciate that 5.06(E) has been amended to remove the prohibition against UOOMs treating "different controllers differently", which arguably undercut the entire purpose of the UOOM; by their definition technologies that facilitate global opt-outs are "disadvantaging" some segment of controllers by limiting their processing of data. For example, a consumer may want to use a certain UOOM that specifically opt-outs them from data brokers (or may configure a general purpose UOOM to only target data brokers); in that case, a consumer (and their agent) should be empowered to only send opt-out requests to data brokers.

However, we remain unsure about what "self-dealing" is prohibited in that same section of the 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 other tracking. In any event, more clarity as to what constitutes prohibited "self-dealing" would be helpful.

Finally, Section 5.06(B) repeats the counterproductive requirement that UOOMs specifically invoke Colorado specific rights already discussed in Section 5.02 and Section 5.03.

Section 5.07 System of Recognizing Universal Opt-Out Mechanisms

In our comments to the Department of Law upon the release of the first round of rules, Consumer Reports noted that we did not believe that Section 5.07(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" was necessary or helpful. We are glad to see that this requirement has been moved to the list of additional factors that the Colorado Department of Law may consider when determining which UOOMs to recognize. As we noted at the time, it may not be practical for all UOOMs, such as those for closed systems, to comply with these requirements and, by the same token, UOOMs designed for the open web may not be directly transferable to other environments either. Allowing the Department of Law to make a fact and context specific determination whether a given UOOM was developed using appropriately open principles and available on reasonable terms is a much more sensible approach.

Section 5.08 Obligations on Controllers

We are pleased that the Department of Law has revised Section 5.08(D) to remove the allowance that controllers could require consumers to login in order to authenticate themselves as a condition of recognizing their use of a UOOM. 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.

Importantly, the CPA states that a controller may authenticate the residency of the user sending a UOOM — not the identity. We urge the Department of Law to go further and 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. Companies commonly use IP targeting to serve advertisements based on consumers' precise location. Surely those same companies have the capability to use IP addresses to assess the legitimacy of an opt-out request.

We previously recommended revising Section 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 Section 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 Sections 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 Section 5.08(A)(1) 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.

Section 5.08(E) of the Draft Rules states that companies "may" indicate compliance with an opt-out preference signal. 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.

Alternatively, as we suggested in our August 2022 comments, 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.[8] This

[8] See Section I(D), 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),

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 6.05 Bona Fide Loyalty Programs

We are concerned that the Revised 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.

To put it simply, loyalty programs should be construed as those that reward consumers for their loyalty to a given service, i.e. using that service consistently instead of another service that they could choose. Patronage is the benefit that controllers receive from consumer loyalty. Discounts or other rewards are the benefit that consumers receive for their loyalty. Loyalty programs should not be confused with other mechanisms by which controllers extract revenues from consumers beyond what they already do in operating the service, such as through data sales and advertising.

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, Section 6.05 should clarify that exercising opt-out rights related to data sales or targeted advertising should never (or almost never)[9] 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.

---

https://advocacy.consumerreports.org/wp-content/uploads/2022/08/Colorado-rulemaking-input-summer-2022.pdf

[9] 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, Section 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 Section 6-1-1308(1)(c)(II) of the law. We recommend these sections be deleted, and the definitions of "bona fide loyalty program" and Sections 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.

Section 7.05 Consent After Opt-Out

As mentioned earlier, due to the ambiguous definition of bona fide loyalty program, 7.05(D) creates a loophole whereby controllers can request consent after a consumer has opted out of a processing purpose so long as they connect the processing of the consumer's data to the

provision of the program, however spurious that connection may be. For example, some controllers may interpret any data sale as necessary to the provision of a loyalty program, claiming that the service would be more expensive without the data sales. In reality, no data sales or targeted advertising supports a loyalty program under any reasonable understanding of that term.

Rule 9.04 Opting Out of Profiling in Furtherance of Decisions That Produce Legal or Similarly Significant Effects Concerning a Consumer

We are disappointed that the Department of Law has significantly diminished the reach of the right to opt out of profiling in the rules. According to Section 6-1-1303(20) of the CPA, "profiling" means *any* form of automated processing of personal data to equate, analyze, or predict a person's economic situation, health, personal preferences, interests, reliability, behavior, location or movements. However, the rules create a sub-category of automated processing, called "Human Involved Automated Processing," which is exempt from the right to opt out of profiling, so long as a human "(1) engages in a meaningful consideration of available data used in the Processing as well as and any output of the Processing and (2) has the authority to change or influence the outcome of the Processing."

The terms "meaningful" and "influence" in this subsection remain undefined and grant controllers far too much leeway to simply insert a human into the automation process and claim that the person had a meaningful role and was able to influence the processing, thus freeing them of their obligation to allow for opt-outs. In practice, a growing corpus of scholarship has found that humans, even those technically empowered to intervene in automated processes, often cannot do so effectively.[10] This can occur for a multitude of reasons, but perhaps most vexingly of all is the "black box" problem, where a human may indeed consider the data used in the processing and have the authority to change a result once the processing occurs, but simply possesses no understanding of how the automated process arrived at the conclusion that it did. This problem plagues even the most technically-attuned humans in the loop, including engineers of the systems themselves, and will only worsen as automated processes become more sophisticated.[11] Therefore, it is highly likely that the act of carving up automated processing into two chunks (an action not supported by the text of CPA), one of which is exempted from a key requirement of the law ostensibly due to the enhanced human safeguards in place, will strip consumers of their rights without any sort of countervailing protection.

****

[10] See, e.g., Brennan-Marquez, Kiel and Susser, Daniel and Levy, Karen, Strange Loops: Apparent versus Actual Human Involvement in Automated Decision-Making (October 2, 2019). 34 Berkeley Technology Law Journal 745–771 (2019), https://ssrn.com/abstract=3462901

[11] Will Knight, The Dark Secret at the Heart of AI, MIT Technology Review, (April 11, 2017), https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/

Thank you very much again for the opportunity to provide feedback on the Revised Draft Rules. 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) or Matt Schwartz (matt.schwartz@consumer.org) for more information.