Before the
Office of the Attorney General
Colorado Department of Law
Denver, CO

In the Matter of:

Colorado Privacy Act Rules-
Universal Opt Out Mechanism
(UOOM) Registry

)
)
)
)

Docket No. 4 CCR-904-3

Comments of the Electronic Privacy Information Center (EPIC)

Electronic Privacy Information Center (EPIC)
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140

Alan Butler, Executive Director
Chris Frascella, Counsel

via electronic submission to coag.gov

December 11, 2023

Table of Contents

Introduction..........1

Feedback on Individual Applications..........2

I. Global Privacy Control (GPC)..........2

II. OptOutCode (OOC)..........4

III. The Opt-Out Machine (TOOM)..........9

Considerations Across Applications..........11

I. Multiple UOOMs..........11

II. Multiple Devices and Multiple Reversions of the End User's Opt-Out Choice..........11

III. Controllers Soliciting Selective Opt-In Consent..........12

Conclusion..........14

Introduction

The Electronic Privacy Information Center (EPIC) is a public interest research center based in Washington, D.C. that was established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[1] EPIC frequently provides comments to federal and state agencies to strengthen privacy and data protection regulations.[2] EPIC respectfully submits these comments in response to the Colorado Attorney General's and the Department of Law's (collectively, the Department's) invitation for comment on the Universal Opt-Out Mechanism (UOOM) shortlist.[3]

Our comments include feedback on each of the three applications that were filed with the Department. We believe that the Global Privacy Control provides the strongest (exemplary) application, that the OptOutCode is a promising application with potential, and that the Opt-Out Machine is an inadequate application inappropriate for Colorado's circumstances.

We have also identified general considerations that we believe the Department should take into account when reviewing the UOOM applications. Where the Department permits consumers to make use of any of several UOOMs, the Department should require companies to accept any

[1] EPIC, *About EPIC* (2023), https://epic.org/about/.

[2] *See, e.g.*, Comments of the Electronic Privacy Information Center, In Re: Colorado Privacy Act Rules, Dkt. No. 4 CCR-904-3 at 20 (Jan. 12, 2023), https://epic.org/documents/colorado-privacy-act-revision-comments/; Comments of the Electronic Privacy Center to the Colorado Department of Law, On Proposed Rulemaking Under the Colorado Privacy Act of 2021 (Aug. 5, 2022), https://epic.org/documents/epic-comments-on-colorado-privacy-act-rulemaking/ [hereinafter "EPIC Aug. 2022 Comments"]; Comments of EPIC et al. to Cal. Priv. Protection Agency (June 8, 2022), https://epic.org/wp-content/uploads/2022/06/GlobalOptOut-Coalition-Letter.pdf; Comments of EPIC and Coalition to Cal. Priv. Protection Agency (Nov. 8, 2021) https://epic.org/documents/comments-of-epic-and-three-organizations-on-regulations-under-the-california-privacy-rights-act-of-2020/; Comments of EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; *see also* Comments of EPIC, *In re* Data Breach Reporting Requirements, WC Docket No. 22-21 (Feb. 23, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10222069458527.

[3] *Universal Opt-Out Shortlist*, https://coag.gov/uoom/ (last visited Dec. 11, 2023).

valid opt-out signal as sufficient. We urge the Department to require the Controller to "remember" each consumer's opt-out preference. The Department should also consider an upper limit on the frequency with which a Controller can ask a consumer to selectively consent (superseding their UOOM preference) and explicitly prohibit a Controller from obtaining selective consent on behalf of other entities.

Feedback on Individual Applications

I. Global Privacy Control (GPC)

We believe that the Global Privacy Control (GPC) meets the standards of the Colorado Privacy Act and that the Department should add GPC to the public list of approved UOOMs pursuant to 4 CCR 904-3, Rule 5.07. The Department should also take the opportunity to recognize Global Privacy Control (GPC) as an exemplary protocol given its privacy-protective structure, the robust testing it has undergone, and its low-impact adoptability by small independent websites.[4]

The GPC not only meets the minimum standards of Rule 5.07:[5] it exceeds them and evaluates favorably under the other factors listed because the GPC is already implemented on a broad scale,[6] including by thousands of small independent websites seeking to minimize development and administrative costs;[7] the GPC has undergone a W3C standardization process;[8] the GPC is free for adoption by manufacturers, Controllers, and Consumers;[9] and the GPC has

[4] This is consistent with EPIC's recommendations from last year. *See* EPIC Aug. 2022 Comments at 14.

[5] Rule 5.07(C) requires a valid UOOM to comply with all of the specifications of Rule 5 and to not create confusion about similarities and differences between UOOMs.

[6] Rule 5.07(D)(1).

[7] *See* Global Privacy Control application for inclusion in Colorado's UOOM registry at 8, https://coag.gov/app/uploads/2023/11/Global-Privacy-Control-Application.pdf [hereinafter "GPC UOOM"]; Rule 5.07(D)(2).

[8] *See* GPC UOOM at 11; Rule 5.07(D)(3).

[9] *See* GPC UOOM at 17; Rule 5.07(D)(4).

been recognized as legally binding in California since January 2021.[10] In fact, the California Attorney General has already announced a settlement with a company that failed to treat GPC signals as opt-out requests.[11]

In terms of protecting privacy, GPC only requires the Controller to read the binary opt-out signal in order to process the user's opt-out request;[12] there is no need to collect additional information from the user. This is ideal from a data minimization perspective, which aligns with our earlier comments to the Department[13] and with Rule 5.08(D).[14]

In terms of ease of adoption, the GPC application notes that the mechanism "is completely free to use for consumers, free for user agents [e.g. browsers such as Brave[15]] to implement, and is designed to be extremely simple for businesses to detect and process."[16] EPIC finds the reported implementation of GPC by 4,000 small independent websites encouraging.

In its application, GPC further notes that it can easily scale to mobile operating systems, payment services, and other Internet of Things platforms,[17] but does not go into greater detail on

[10] *See* GPC UOOM at 11.
[11] *See* id. at 9 (citing Press Release, Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act, State of California Department of Justice, Aug. 24, 2022, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement).
[12] *See* id. at 1, 3, 5.
[13] *See* Comments of the Electronic Privacy Information Center, In Re: Colorado Privacy Act Rules, Dkt. No. 4 CCR-904-3 at 20 (Jan. 12, 2023), https://epic.org/documents/colorado-privacy-act-revision-comments/ ("Put simply, the rules should reinforce Consumers' autonomy when their information is requested and ensure that no more data than necessary is collected to implement the universal opt-out mechanism."); EPIC Aug. 2022 Comments at 17 ("It is important that the implementing regulations do not require controllers to collect additional information from Colorado residents").
[14] Rule 5.08(D) reads: "A Controller may not subject a Consumer to undertake any authentication actions that are unnecessary or unnecessarily burdensome."
[15] *See, e.g.*, GPC UOOM at 6.
[16] *Id.* at 4.
[17] *See* id. at 10.

this point. We hope that GPC will continue to expand so that users can opt out of tracking beyond a single browser.

II. OptOutCode (OOC)

We believe that the Department should ask further questions about the OptOutCode (OOC) and consider approving it as a UOOM at a future date if the Department determines commercial adoption is feasible. It appears that OOC's application oversimplifies some of the implementation challenges it is likely to encounter; although these challenges are not insurmountable, they must be addressed before the Department requires companies to comply with the mechanism. For example, as of iOS 16, special entitlements[18] are required to be able to access the name field OOC suggests using: `UIDevice.current.name`.[19] Similarly, the primary appeal of OOC is its universal applicability;[20] however, OOC's submitted application leaves several key questions unanswered about operating systems, routers, and individual Internet of Things (IoT) devices. Additionally, OOC has not been extensively vetted.[21] As with GPC above we will begin with this point first.

We have reviewed the OOC proposal and believe that the mechanism could provide a way for consumers to opt out of tracking on some devices that are not compatible with GPC or other mechanisms. However, we have not formally vetted the mechanism in terms of its

[18] *See* "com.apple.developer.device-information.user-assigned-device-name", Apple Developer, https://developer.apple.com/documentation/bundleresources/entitlements/com_apple_developer_device-information_user-assigned-device-name (last visited Dec 11, 2023).

[19] *See* OptOutCode, A Privacy4Cars® Universal Opt-Out Concept at 9, https://coag.gov/app/uploads/2023/11/OptOutCode-Application.pdf [hereinafter "OOC UOOM"].

[20] *See* OOC UOOM at 2.

[21] To this point, although EPIC considers OOC to be a potentially promising concept and looks forward to seeing more from the mechanism, OOC's application overstates EPIC's interest and enthusiasm in OOC by characterizing it as "formal support" and "official support" in its application. *See, e.g., id.* at 2, 3, 14, 15, 20.

commercial adoption, its ease of use by controllers, or its review by standards setting bodies. Per the OOC application, Privacy4Cars has performed extensive testing over the past two years and will imminently be releasing an application and a software development kit (SDK) to make it easier for developers to adopt OOC.[22] This suggests that OOC is not a mere hypothetical solution. However, OOC has not been subject to the same type of rigorous testing and design review as GPC, which has been subject to widespread implementation, standardization, and enforcement.[23] On its own, this does not undermine the validity of the OOC spec, but it is an important consideration to acknowledge.

One specific issue that deserves consideration is OOC's requirement that Controllers scan device names, as this raises potential questions of privacy impact, consumer confusion, enforcement, and future compatibility. For OOC's UOOM to function, a Controller must read the device name. The OOC application suggests this potential privacy issue could be mitigated by having the Controller deploy code to only read the first three characters of the device name.[24] This is less privacy-protective than the binary signal of GPC; however, it might be possible to implement this in a way that minimizes privacy risk.[25] Even assuming this could be achieved in a way that ensures the full device name is not used or permanently stored, there is still the possibility of consumer confusion in the counterintuitive practice of having to grant an app permission to read the user's device name in order for that app to respect the user's privacy preferences. There are also questions of enforcement. A Controller that uses or stores the device name beyond the scope of checking it for the OOC signal would likely run afoul of Rule

[22] *See* id. at 7, 13-14.
[23] *See* GPC UOOM, *supra* notes 7-9.
[24] *See* OOC UOOM at 7.
[25] Although this is not without its enforcement challenges, noted below.

5.08(D); however, Controllers would be entrusted to implement this accurately and the burden would be on the Department to enforce violations. We note that there have been compliance issues with the "_nomap" example provided in OOC's application,[26] but we believe the Department's enforcement of its own regulations would yield a different result than Google's enforcement of its own policy. In terms of future challenges, changes like iOS 16's device name access permissions are likely to recur. A mechanism premised on reading device name seems unlikely to be "future-proof" as OOC claims.[27] These issues are not necessarily fatal flaws that preclude OOC from ever serving as a UOOM, but they must be more fully addressed before the Department approves OOC as a mechanism.

In terms of ease of adoption, OOC has clearly thought through much of the consumer side of implementation. In its application, OOC identifies that it is simple for a user to change their device name,[28] notes that it is developing tools to make it even easier for consumers who might not go through the normal sequence of steps required to change their device name,[29] and acknowledges that consumer awareness will be an important component to widespread adoption of the mechanism.[30] We note that an SDK in particular could significantly extend the impact of OOC across apps.[31] OOC would be free to consumers.[32] Additionally, there may be some user

[26] *See, e.g.*, Joel Reardon, *What the Huq?*, AppCensus Blog (Oct. 25, 2021), https://blog.appcensus.io/2021/10/25/what-the-huq/.
[27] *See* OOC UOOM at 17.
[28] *See* id. at 2-3, 6-7, 20.
[29] *See* id. at 7, 13-14.
[30] *See* id. at 14.
[31] *See* id.
[32] *See* id. at 1.

confusion about which device needs to be renamed under what circumstances.[33] We address a related issue of guests on an OOC-enabled network in the penultimate paragraph of our comments on OOC's application.

The bigger 'ease of adoption' questions raised by the OOC application pertain to the Controller side of adoption. The OOC application assumes that reading the device name is an established and future-proof IT protocol.[34] We do not expect that reading only the first three characters rather than the entirety of the device name significantly undermines this point, but as noted above reading the device name itself presents implementation challenges and may not be future-proof. Additionally, while OOC's application includes code examples for Android, Windows, and iOS,[35] and notes that browsers would be able to read OOC,[36] there is no explanation of how Controllers would comply if OOC were deployed in circumstances that don't involve a browser or one of the listed operating systems, as could be the case with an IoT device. OOC also proposes that its mechanism could transmit an opt-out signal for all devices on a network by modifying the name of the router's service set identifier (SSID);[37] this would likely work for upstream applications, downstream devices, etc. ("applications") that read the network name, but it is less clear whether it would work for applications that read device name without

[33] For example, OOC's application suggests a renamed Wi-Fi router would protect a SmartTV connected to the network, and that similarly a fitness watch would be protected by the renamed corresponding smartphone. *See* OOC UOOM at 13. However, an end user may not think to rename their SmartTV or other device (e.g., gaming console, portable speaker) before connecting it to a different network.

[34] *See, e.g.*, OOC UOOM at 3, 4, 6, 7, 12, 17, 20; specific examples id. at 8-11.

[35] *See* id. at 7-11; but note iOS 16 issue discussed above, *supra* note 18.

[36] *See* OOC UOOM at 4, 10.

[37] *See* id. at 2.

reading the network name.[38] Notably, SSID has also been abused as a backdoor to infer location information in the past.[39]

As a final point about adoption of OOC, we acknowledge that the end user interface of some devices and applications (as compared with those of some web browsers) may make it more difficult for end users to alter selective opt-in preferences (e.g. 'whitelisting' individualized Controllers or revoking selective consents individually) while using OOC. This is not a flaw with OOC but is a function of the underlying ecosystem. We do not believe this obstacle should preclude the Department from approving OOC as a UOOM for non-web browser contexts, but it is worth noting.

What EPIC finds most encouraging about OOC is the theoretically universal nature of its applicability. Although OOC was developed in response to issues with cars collecting and sharing information from connected devices,[40] by design OOC could potentially apply to any device connecting via Wi-Fi and most via Bluetooth.[41] To work in this way, the device would need to allow for the end user to rename it (and again with caveats about user education and user expectation regarding which devices need to be renamed in which circumstances, e.g., SmartTV vs. Wi-Fi router). There may be complications with guests connecting to a network utilizing OOC, in that a guest's device may not include the OOC but the host router they are connecting through will. Similarly, if the owner of a vehicle implemented OOC in their car, but a passenger

[38] There are also potential questions regarding whether IoT devices might require software or firmware updates for third-party applications to be able to read the modified name.
[39] *See, e.g.*, Stacey Gray, *A Closer Look at Location Data: Privacy and Pandemics*, Future of Privacy Forum (Mar. 25, 2020), https://fpf.org/blog/a-closer-look-at-location-data-privacy-and-pandemics/ ; David Kofoed Wind, et al., *Inferring Stop-Location from WiFi*, PLoS One 11(2) (2016), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4763164/.
[40] *See* OOC UOOM at 1-2.
[41] *See, e.g.*, id. at 2, 17, 19.

who actively chose not to implement OOC connects their smartphone to the driver's car, which should take priority? If the consumer is renting a vehicle with an infotainment system and connects their smartphone, which device's signal should take priority? For this and related reasons, Controllers may challenge whether consumer opt-out preferences should be recognized at a network level. We urge the Department to clarify that opt-out signals are still valid in situations in which multiple devices or users connect to the internet through the same device or service, such as guests connecting their smartphones to the internet through their host's Wi-Fi router, or passengers connecting their smartphones to the driver's vehicle, or multiple family members using the same web browser on a shared home computer.

We encourage the Department to request additional information concerning OOC such as the logistical challenges of requiring Controllers to scan device names, the precise range of systems (e.g., operating systems, browsers, etc.) that can comply with OOC immediately, and the increased privacy risks resulting from enabling a universal opt-out mechanism through reading device name.

III. The Opt-Out Machine (TOOM)

The Opt-Out Machine (TOOM) proposes to take upon itself the burden consumers would otherwise face of identifying and communicating individually with every data broker that has their data. We do not believe TOOM is an optimal universal opt-out mechanism under the Colorado Privacy Act for several reasons.

TOOM's founders indicate that it is a startup, that its proposal is not yet widely adopted, but that it has been tested in the marketplace and received some feedback from both data brokers and consumers.[42] They also indicate that they will share a scorecard of data broker compliance with TOOM requests in the future.[43]

It appears that TOOM would require a profile be kept of each end user so that their request would be honored across devices;[44] at a minimum it explicitly would require the user's mailing address.[45] This raises privacy concerns, especially in comparison to the other two shortlisted UOOMs which do not raise such concerns.

In terms of adoption, there is a monetary cost associated with consumer use of TOOM, although its founders indicate that there may be circumstances in which it would be offered for free.[46] EPIC notes that charging consumers to be able to prohibit the sale or sharing of their data, even at an ostensibly low cost, amounts to requiring users to pay for privacy. On the Controller side, companies would need to monitor their email and comply with each request.[47] It is conceivable that Controllers could automate this process, but TOOM does not explicitly suggest this in its application nor provide examples of what this might look like.

Per its application, TOOM indicates that it proactively and automatically sends requests to brokers and may incorporate bots to expedite this process, and that scaling up the solution would not result in additional burdens to consumers.[48] As with OOC's use of SDKs, bundling TOOM with other services could extend its impact.[49]

[42] *See* OOC UOOM at 4-5.
[43] *See i*d. at 6.
[44] *See* Opt Out Machine Application at 4, https://coag.gov/app/uploads/2023/11/Opt-Out-Machine-Application.pdf [hereinafter TOOM UOOM].
[45] *See* TOOM UOOM at 4.
[46] *See* id.
[47] *See* id. at 3, 4, 6.
[48] *See* id. at 3.
[49] *See* id. at 4.

Considerations Across Applications

In addition to feedback on the content of the specific UOOM application materials, we also highlight considerations the Department may wish to keep in mind as it evaluates the applications. These include managing multiple UOOMs, resolving seemingly contradictory signals from end users (whether users implement the same UOOM across all devices, applications, and browsers, or different UOOMs), and limitations on Controllers seeking selective opt-in consent (to supersede UOOM signals).

I. Multiple UOOMs

At this time, we do not support the Department approving multiple UOOM applications before its January 1, 2024 deadline. However if in the future the Department approves multiple UOOMs, it may need to address how those mechanisms interact. The simplest and most consumer-friendly regime would be to interpret any valid opt-out as sufficient across all mechanisms. By initial default, end user silence about data sharing is presumed to be opting in, even if in reality the consumer would opt out of data sharing but is unaware that they can. Accordingly, it would be inappropriate to disregard one or more valid opt-out signals merely because the consumer did not implement every possible valid UOOM. Similarly, if a consumer whitelists a website or application to opt in to data sharing through one UOOM but communicates an opt-out without selective consent through a different UOOM, the opt-out should take priority. That said, this scenario may justify the Controller prompting the consumer to also whitelist the website or application via the other UOOM. (This would triggered by the end user already having whitelisted the service; it would not be triggered by the default opt-in).

II. Multiple Devices and Multiple Reversions of the End User's Opt-Out Choice

The same consumer may enable an UOOM on one device or browser but not enable it on another. Rule 5.09(B) requires that a Controller shall not interpret the absence of a UOOM signal as consent to opt back in after the consumer previously utilized a UOOM.[50] To the extent that it does not require a Controller to attempt to identify a specific user or household,[51] we urge the Department to require Controllers to "remember" each consumer's designated preference to opt out. As discussed by GPC in its application, to the extent a user is logged in or otherwise authenticated, the Controller should apply the opt-out instruction universally.[52]

III. Controllers Soliciting Selective Opt-In Consent

The Department has indicated that mechanisms that cause consent fatigue or obstruct or degrade the end user's experience cannot result in valid selective consents (i.e., individualized consents that would supersede an UOOM signal).[53] The Department has also offered examples that illustrate valid and invalid invitations to opt in to data sharing in the context of a website.[54] We urge the Department to consider issuing guidance as to how a device or software application independent from a website might comply with these requirements and whether additional examples or parameters may be helpful (for instance, an upper limit on how frequently an entity may solicit a selective consent).

Beyond data sharing, we additionally urge the Department to limit a Controller's ability to obtain selective consent to the immediate website, application, or device and not permit a Controller to obtain selective consent that supersedes an UOOM signal on behalf of other entities, including of other affiliates or subsidiaries of the Controller. Per Rule 5.09(A), the CPA

[50] *See also* Rule 7.05, which requires that a consumer affirmatively opt in to data sharing after sending an opt out signal, and Rule 7.07, which requires that revoking or withdrawing selective consent must be through a similar interface as consent was obtained and be as easy and within a similar number of steps.
[51] *See* EPIC Aug 2022 Comments at 17 ("It is important that the implementing regulations do not require controllers to collect additional information from Colorado residents and do not allow controllers to undermine the purpose of the universal opt-out provision").
[52] *See* GPC UOOM at 10.
[53] *See* Rule 7.05(B).
[54] *See, e.g.,* Rule 7.05(E,F).

allows a Controller to obtain consent to processing post-UOOM signal if it complies with the consent requirements of C.R.S. § 6-1-1306(1)(a)(IV)(C), and 4 CCR 904-3, Rule 7.05. The statute indicates that “a controller may enable the consumer to consent, through a web page, application, or a similar method, to the processing of the consumer's personal data for purposes of targeted advertising or the sale of personal data”[55]—it does not stipulate that it must be the Controller’s own webpage or application that solicits the selective consent.

The regulations indicate that Consumers must have the ability to separately consent to each specific purpose for processing personal data[56]—this addresses data sharing, but it says nothing about selective consent obtained by Controller A on behalf of Controller B. Indeed, presumably so long as Controller B’s identity is listed on Controller A’s selective consent mechanism, the acquisition of selective consents on behalf Controller B by Controller A would be allowed under the current rules.[57] This should be explicitly prohibited; each selective consent should be obtained separately. One way the Department might accomplish this is by finding such a mechanism to be manipulative design, as Rule 7.03(F) establishes that consents obtained through dark patterns are invalid. The Department should not permit companies to obtain selective consents that supersede UOOM signals on behalf of other entities, including their own affiliates and subsidiaries.

[55] C.R.S. § 6-1-1306(1)(a)(IV)(C).
[56] *See* Rule 7.03(D)(1).
[57] *See* Rule 7.03(E)(1)(a).

This is consistent with recent statements by the Federal Trade Commission[58] and Federal Communications Commission[59] regarding obtaining consent to receive telemarketing calls under the Telemarketing Sales Rule and the Telephone Consumer Protection Act. It also likely aligns with consumer expectations regarding giving individualized consent, especially in light of how seemingly unrelated companies may in fact be affiliates or subsidiaries of one another.[60] The Department's regulations require the Controller provide their name[61] and provide consent separately for distinct specific purposes[62] but do not indicate whether the Controller may provide the name of multiple Controllers in its request for selective consent from the consumer. In sum: we ask the Department to clarify that one entity (Controller A) may not obtain selective consent from a consumer on behalf of a second entity (Controller B) that supersedes that consumer's UOOM preferences, which is a separate inquiry from whether Controller A respects the consumer's UOOM signal regarding the sale to Controller B of data collected by Controller A.

Conclusion

We encourage the Department to approve GPC before the Department's January 1, 2024 deadline, to seek additional information from OOC for a potential later approval date, and to

[58] *See* 73 Fed. Reg. 51,163, 51,182 (Aug. 29, 2008) ("[T]he Commission emphasizes that a consumer's agreement with a seller to receive calls delivering prerecorded messages is nontransferable. Any party other than that particular seller must negotiate its own agreement with the consumer to accept calls delivering prerecorded messages. Prerecorded calls placed to a consumer on the National Do Not Call Registry by some third party that does not have its own agreement with the consumer would violate the TSR . . . .").

[59] *See* FCC Fact Sheet, Combatting Illegal Text Messages 1 (Nov. 22, 2023), https://docs.fcc.gov/public/attachments/DOC-398661A1.pdf ("[This Order would c]lose the lead generator loophole by making unequivocally clear that comparison shopping websites must get consumer consent one seller at a time, and thus prohibit abuse of consumer consent by such websites").

[60] *See* Fed. Trade Comm'n, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* i-iv (2021), https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major- internet-service-providers.

[61] *See* Rule 7.03(E)(1)(a).

[62] *See* Rule 7.03(D).

decline to approve TOOM unless it undergoes substantial revision. We thank the Department for the opportunity to provide this input.

Sincerely,
Alan Butler, EPIC Executive Director
Chris Frascella, EPIC Counsel