409 7th Street, NW Suite 250
Washington, DC 20004

Submitted electronically via: https://coag.gov/uoom/

December 11, 2023

Phil Weiser
Attorney General
Colorado Department of Law
Ralph L. Carr Judicial Building
1300 Broadway, 10th Floor
Denver, CO 80203

Re: Universal Opt-Out Shortlist

Dear Mr. Weiser:

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to provide comments on the shortlist of Universal Opt-Out Mechanisms ("UOOMs")[1] being considered by your office to enable consumers to opt out of sales and/or targeted advertising under the Colorado Privacy Act (the "CPA")[2] and its implementing regulations (the "Regulations").[3]

Founded in 2000, the NAI is the leading non-profit, self-regulatory association for advertising technology companies. For over 20 years, the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining the highest industry standards for the responsible collection and use of consumer data for advertising. Our member companies range from large multinational corporations to smaller startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and enhancing consumer trust. The NAI Code of Conduct (the "NAI Code")[4] has long promoted these standards for its members, and the NAI membership demonstrates its commitment to them by undergoing required annual privacy reviews by NAI staff attorneys.

---

[1] https://coag.gov/uoom/.
[2] *See* Colo. Rev. Stat. § 6-1-1306(1)(a) (setting forth consumer rights to opt out of "sales" and "targeted advertising" and requiring controllers to honor consumer opt-out choices expressed through universal opt-out mechanisms approved by the Colorado attorney general).
[3] *See generally* Colo. Code Regs. § 904-3 (2023).
[4] Network Advertising Initiative, 2020 NAI Code of Conduct (2020) https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf [hereinafter "NAI Code"].

The ability of consumers to easily opt out of the use of their personal data for certain advertising purposes is crucial both for consumer privacy and for the health of the digital advertising ecosystem. It enables consumers to exercise meaningful control over how their personal data are used and increases trust in free and ad-supported products and services consumers have come to rely on and enjoy. The NAI has long provided consumers with an easy-to-use and comprehensive set of methods to opt out of Tailored Advertising,[5] which gives the NAI a unique perspective on the potential benefits and challenges of implementing the UOOMs your office included on the shortlist. Below, we provide comments on the overarching set of criteria the DoL will use to assess feasibility of UOOMs, as well as feedback on each of the three proposed UOOMs under consideration.

In summary, the NAI recommends the following with respect to the candidate UOOMs included in the shortlist:

- **Global Privacy Control**: The NAI would support the inclusion in the initial list of approved UOOMs only specific implementations of GPC that demonstrably satisfy the Consumer Choice Principle (outlined below) and meet the requirements set forth in the CPA and the Regulations. The technical specification for the GPC itself, though, should not be included in the initial list independently of specific implementations because the specification alone does not (and as currently specified, cannot) demonstrate compliance with the Consumer Choice Principle.
- **OptOutCode**: The NAI opposes the inclusion of OptOutCode in the initial list because the applicant did not go through the process of consulting with a broad base of stakeholders as urged by the DoL, which in effect denied industry groups like the NAI the opportunity to provide meaningful input on its design and implementation. While the OptOutCode deserves careful evaluation because it addresses internet-connected devices outside of the web-browser environment, the applicant's failure to follow the process articulated by the DoL prevented the applicant from receiving or considering input on various implementation issues that may arise if OptOutCode is included in the initial list. Further engagement with industry stakeholders, including the NAI, could strengthen a future submission of OptOutCode as the list of UOOMs is intended to be updated "periodically."
- **Opt-Out Machine**: The NAI opposes the inclusion of the Opt-Out Machine in the initial list of UOOMs because the application represents a confusion between two distinct concepts in the CPA – that of a UOOM and that of an authorized agent. Based on the application materials, we view the Opt-Out Machine as an authorized agent service that controllers are already required to allow for if the service demonstrates that it meets the requirements for authorized agents under the CPA. Including it on the list of UOOMs

[5] Within the context of the NAI's 2020 Code of Conduct, Tailored Advertising "is the use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device." NAI CODE § I.Q. The NAI Code's definition of Tailored Advertising is similar to the definition of "Targeted Advertising" under the CPA. *See* COLO. REV. STAT. § 6-1-1303(25). For more information on how consumers may opt out of Tailored Advertising, *see* https://optout.networkadvertising.org/.

would be duplicative and also would invite confusion about the important consumer verification and authorization requirements that pertain to authorized agents.

I. Criteria for Assessment of all UOOMs

Our comments below reflect not only our assessment of the merits of each shortlisted proposal based on the NAI's experience developing and operating consumer opt-out mechanisms for 20 years, but also the explicit standards set forth in the CPA, the Regulations, and the application issued by the Colorado Department of Law and your office (the "DoL") for prospective UOOMs (the "Application").[6] In particular, our comments focus on two key, general principles established in those materials – the Consumer Choice Principle and the Collaboration Principle – as well as other specific issues unique to each applicant.

A. The Consumer Choice Principle

One primary principle guiding the DoL's adoption of any UOOMs that is reflected in the CPA, the Regulations, and the Application, is that a UOOM must represent a Consumer's authentic choice to opt out of sales and/or targeted advertising (collectively, the consumer's choice to "Opt Out").[7] More specifically, the Regulations require UOOMs to represent a Consumer's "affirmative, freely given, and unambiguous choice" to Opt Out[8] and prohibit any UOOM from being "the default setting for a tool that comes pre-installed with a device, such as a browser or operating system."[9] We refer to these considerations together as the "Consumer Choice Principle."

The Regulations also provide helpful examples of hypothetical Opt-Out Mechanisms that would, and would not, constitute valid UOOMs based on the application of the Consumer Choice Principle. Regardless of the technical signal used to store or transmit an Opt-Out signal, the Regulations make clear that the user interface employed by a valid UOOM must represent an authentic consumer choice; and that the hypothetical illustrating a signal sent by default without ever asking the consumer to enable such a signal does not represent the consumer's "affirmative, freely given, and unambiguous choice" to Opt Out.[10] In other words, this type of signal implementation would violate the Consumer Choice Principle and would not constitute a valid UOOM.

---

[6] Colorado Dept. of Law, Colorado Privacy Act: Application for Inclusion in Colorado's Public List of Universal Opt-Out Mechanisms (Oct. 5, 2023) (hereinafter, the "Application"), https://coag.gov/app/uploads/2023/10/UOOM-Application-copy_FINAL-10.3.23.pdf..

[7] Colo. Rev. Stat. § 6-1-1306(1)(a) (2023).

[8] Colo. Code Regs. § 904-3 Rule 5.03(B) (2023) ("A valid Universal Opt-Out Mechanism must represent the Consumer's affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for the purposes listed at C.R.S. § 6-1-1306(1)(a)(IV)(A) and (B). Controllers are not obligated to honor Consumer rights requests for purposes other than those listed at C.R.S. § 6-1-1306(1)(a)(IV)(A) and (B) when transmitted through a Universal Opt-Out Mechanism.").

[9] Colo. Code Regs. § 904-3 Rule 5.04(A) (2023).

[10] *Id.* Rule 5.04(A)(1).

In our comments on the shortlisted UOOM applications below, we highlight the importance of the user interface as an integral component of any valid UOOM, because technical signal specifications presented independently of a user interface (or, in some cases, independently of any marketing materials or user guides)[11] cannot satisfy the Consumer Choice Principle and therefore do not meet the requirements for a UOOM set forth in the CPA and the Regulations.

B. The Collaboration Principle.

The digital advertising ecosystem that powers free and low cost ad-supported media for consumers involves the interplay of signals and other technical infrastructure among Internet-connected devices, web browsers, device operating systems, specific digital properties like websites and apps, and the advertising technology providers that facilitate the selection and delivery of ads to those digital properties. UOOMs have the potential to help consumers express their privacy choices throughout that ecosystem, but in order for them to do so successfully each part of the ecosystem must be able to recognize, parse, honor, and transmit the signal component of any UOOM. In other words, any successful UOOM must be the result of a collaborative process that takes into account considerations raised by all stakeholders in the Internet ecosystem. We refer to this as the "Collaboration Principle." The DoL highlighted the importance of the Collaboration Principle when it "strongly urge[d] organizations and entities to work collaboratively in groups to propose UOOMs and to obtain broad pre-submission input from diverse sets of stakeholders" and included breadth of participation in the development process and solicitation and consideration of third-party comments as evaluation criteria for UOOM applications.[12]

Without respecting the Collaboration Principle by engaging in a multi-stakeholder development process and planning for interoperability, a legally-binding UOOM could upset consumer expectations (for example, if the signals carrying their Opt-Out choices are missed, dropped, or misinterpreted due to a lack of interoperability), and it could lead to unfair compliance burdens on participants in the ecosystem that never had the opportunity to contribute to the development of those signals or plan for their impacts.

[11] *Id.* Rule 5.04(A)(2).
[12] Application § II.

II. Comments on Applications for Universal Opt-Out Mechanisms on the Shortlist

The NAI is providing comments below on each of the applications for UOOMs included by the DoL on its shortlist. Our comments raise considerations with respect to the Consumer Choice Principle and Collaboration Principle discussed above, as well as other specific technical and legal considerations raised by the different applications.

A. Global Privacy Control (GPC)

The NAI supports inclusion of specific implementations of the Global Privacy Control (GPC) in the initial list of approved UOOMs, but opposes inclusion of the GPC signaling specification independently of specific implementations.

GPC is an open-source technical specification for a signal set at the web-browser level. According to the applicants submitting GPC for consideration as an UOOM, it is "designed to allow Internet users to notify business of their preference not to have their data be sold or shared, or used for cross-context behavioral advertising."[13] GPC functions by attaching to HTTP requests as the Sec-GPC request header and displaying a value of "1" if GPC is enabled.[14] When GPC=1, this is meant to represent a consumer's choice to Opt Out.

GPC is already seeing a level of uptake in the market and has been recognized by California regulators, making it an important candidate for inclusion in the initial list of approved UOOMs. In January of 2021, then California Attorney General Xavier Beccera stated on his Twitter account that the California Consumer Privacy Act (CCPA) "requires businesses to treat a user-enabled global privacy control as a legally valid consumer request to opt out of the sale of their data" and that GPC satisfies the legal requirements set out by the law.[15] Further, in August of 2022, California Attorney General Rob Bonta announced the first public CCPA enforcement action against Sephora, citing the company's failure to process consumer opt outs from the sale of personal information via GPC.[16]

However, despite California's embrace of GPC, it still presents implementation difficulties. If GPC displays a value of "1", for example, this does not by itself reflect any information about how a choice to Opt Out was presented to a consumer, or whether such a choice was presented at all (*i.e.* if it is a default setting). As such, the GPC technical specification alone is not capable of respecting the Consumer Choice Principle in a way that complies with the CPA and the

[13] Global Privacy Control, Application for Inclusion in Colorado's UOOM Registry at 1 (hereinafter "GPC Application"), https://coag.gov/app/uploads/2023/11/Global-Privacy-Control-Application.pdf.
[14] *Id*.
[15] @AGBecerra, Twitter (Jan. 28, 2021, 12:56 PM) https://twitter.com/AGBecerra/status/1354850758236102656; ("#CCPA requires businesses to treat a user-enabled global privacy control as a legally valid consumer request to opt out of the sale of their data. CCPA opened the door to developing a technical standard, like the GPC, which satisfies this legal requirement & protects privacy.").
[16] *People of the State of California v. Sephora USA, Inc.*, San Francisco Superior Court Case No. CGC-22-601380, ¶ 12.

Regulations. Instead, the user interface controlling whether GPC is turned on or off by default, as well as how any choice is presented to consumers, depends entirely on how web browsers and browser extensions that use GPC choose to implement the user interface independently of the GPC technical specification.[17]

The Regulations themselves illustrate the importance of user interfaces independently of technical specifications when they present examples of two different user interfaces a web browser could employ with respect to a UOOM, only one of which respects the Consumer Choice Principle.

> *Example 1:*
>
> "The browser sends a Universal Opt-Out mechanism signal by default and never asks the Consumer to enable this setting. The Consumer's decision to use this browser does not represent the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism because it is a default choice."[18]
>
> *Example 2:*
>
> "The first time a Consumer runs a browser . . . the operating system asks the Consumer specifically and clearly whether they want to opt out of the Sale of their Personal Data using a Universal Opt-Out Mechanism signal when using the browser . . . No choice is pre-selected, meaning the Consumer is forced to decide. The Consumer's decision to select "yes" to enable the signal to opt out of the Sale of Personal Data represents the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism."[19]

If we assume that the technical specification used in both examples above is GPC, this goes to show that if GPC were used as the signaling mechanism in Example 1, it would not comply with the requirements for UOOMs because it would be sending an Opt Out signal that does not communicate a consumer's authentic choice to Opt Out.[20] Without assurance that the user interface implementing GPC includes proper notice, choice architecture, and is not a default setting, GPC itself cannot be considered a valid UOOM that satisfies the Consumer Choice Principle.

The GPC Application actually presents several distinct web browsers and browser extensions that support GPC,[21] and highlights one screenshot of the user interface employed by the Firefox

---

[17] Colo. Code Regs. § 904-3 Rule 5.03(A) (2023).
[18] *Id.* Rule 5.04(A)(1).
[19] *Id.* Rule 5.04(A)(2).
[20] *See, e.g.,* Colo. Rev. Stat. 6-1-1313(2)(c) (requiring the DoL "[not to] adopt a mechanism that is a default setting, but rather, clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt out").
[21] *See* GPC Application at 2 (listing Privacy Badger, DuckDuckGo, Firefox, and Brave).

web browser that the applicants say allows consumers to "enable GPC via a checkbox in the settings[.]"[22] However, the GPC application also acknowledges that "specific [GPC] implementations about user interfaces are made by implementing [browsers or browser extensions]." This suggests that different implementations of GPC may or may not respect the Consumer Choice Principle depending on how they are presented to consumers.

To address this issue, the NAI recommends that the DoL only approves specific implementations of GPC that it determines actually do satisfy the Consumer Choice Principle. The DoL should not approve GPC as a UOOM without reference to specific implementations. The GPC Application did not provide detailed information about the user interfaces of the different implementations it mentions; however, the DoL could consider evaluating some or all of the implementations mentioned and making individual determinations as to whether each implementation meets the requirements for a valid UOOM. Alternatively, the specific browsers and extensions that provide this functionality (e.g., Brave, Firefox, etc.) could submit their own implementations for review.

Approving as UOOMs only those specific implementations that the DoL has found meet the requirements for valid UOOMs would help controllers avoid uncertainty as to whether a UOOM they encounter represents an authentic consumer choice. However, this approach would not completely resolve that uncertainty. For instance, the GPC specification itself only conveys information about whether the choice mechanism is turned on or off (GPC=1 or GPC=0). However, the signal transmitted by the GPC does not currently encode information about the source of the GPC signal (*i.e.*, whether the signal originated from an implementation that respects the Consumer Choice Principle or not). Therefore, approving specific implementations of GPC at this time, while better than approving the GPC as such, does not entirely eliminate the risk that controllers may encounter GPC=1 signals that do not represent authentic consumer choices, because un-approved implementations may still remain or be introduced into the market.

To further resolve this uncertainty, the NAI recommends that the DoL consider, when evaluating specific GPC implementations, whether they provide a way for information about *which* implementation is being used to send the GPC signal. For example, information about a web browser (browser type and version) is often included in the header of HTTP requests in the form of user agent strings. This type of information could further assist controllers in determining whether a GPC signal originated from a valid UOOM.

[22] *Id*.

B. OptOutCode

The NAI opposes inclusion of OptOutCode ("OOC") in the initial list of approved UOOMs because the applicant did not adhere to the Collaboration Principle or provide evidence of compliance with the Consumer Choice Principle; however, the NAI invites further discussion of the OOC proposal to assess technical feasibility and to allow input from industry stakeholders.

OOC is a proposal for a UOOM intended to work outside of the web-browser environment and enable consumers to signal Opt Out choices in connection with other internet-connected devices (such as mobile phones, mobile apps, connected TVs, WiFi routers) to the extent users can add the 'O$S' prefix to the name of those devices. However, as explained in more detail below, the current OOC Application[23] is deficient because (1) the applicant did not adhere to the Collaboration Principle; (2) the lack of adherence to the Collaboration Principle leaves a number of important questions about the implementation of OOC unanswered; and (3) the applicant provided no evidence of adherence to the Consumer Choice Principle. We address each of those deficiencies in more detail below.

The NAI recognizes the importance of UOOM approaches that extend beyond the web-browser environment, which the OOC proposal purports to do. However, we have not had the opportunity to engage or evaluate it in any depth because the applicant has not solicited or received any input from industry stakeholders. As a procedural matter, we believe that deeper substantive engagement with stakeholders should occur before any UOOM proposal is accepted by the DoL and given the force of law. This also appears to be the intent of the DoL given its emphasis on the Collaboration Principle.

Further, as the regulations provide for "periodic" updates to the list of UOOMs,[24] the applicant could submit the OOC proposal again in the future if it is further developed and matured after a collaborative, multi-stakeholder process.

1. The OOC Proposal Was Not Developed in Adherence to the Collaboration Principle.

According to the OOC Application, OOC was initially developed as a proprietary method used by Privacy4Cars to assist with communicating privacy preferences in vehicles (such as rental or fleet vehicles that may have multiple users).[25] The NAI is not aware of, and the applicant did not assert, any participation from stakeholders such as consumers, developers, publishers, advertisers, or advertising technology companies that would be responsible for reading, honoring, or transmitting the OOC prefix ('0$S') in practice. In other words, the applicant did not adhere to the Collaboration Principle. This is not to say that a process engaging those

[23] OptOutCode, Application for Inclusion in Colorado's UOOM Registry (hereinafter "OOC Application") at 1, https://coag.gov/app/uploads/2023/11/OptOutCode-Application.pdf.
[24] Colo. Code Regs. § 904-3 Rule 5.07(A) (2023).
[25] OOC Application at 1.

stakeholders would not be fruitful – only that it has not occurred. In fact, the NAI and its membership would welcome the opportunity to engage with Privacy4Cars on the OOC proposal for future consideration to address the concerns we raise below, but we cannot support its adoption as a UOOM before any such process has occurred. Further, the NAI has an appropriate venue for that engagement as well as a wide array of industry stakeholders who are well-positioned to assess the OOC proposal in the NAI Legal, Regulatory, and Data Governance Working Group. Our working group stands ready to engage on this proposal and participate in a multi-stakeholder process that could help the applicant satisfy the Collaboration Principle.

Additionally, the DoL included in its criteria for evaluation that applicants should include "results of previous tests or reviews concerning the UOOM."[26] The OOC Application does not reference tests or external reviews conducted; but industry stakeholders should have the opportunity to engage in testing and review and provide meaningful feedback to the applicant and the DoL before the OOC is adopted as a legally binding standard.

2. *The OOC Applicant's Lack of Adherence to the Collaboration Principle Leaves Key Implementation Questions Unanswered.*

The NAI's review of the OOC application revealed numerous implementation issues that could and should have been addressed by the applicant through a multi-stakeholder engagement process, as urged by the DoL and as set forth in our comments above. We raise them here to demonstrate the kinds of issues we would seek to work with the applicant to address before we could consider supporting the OOC proposal.

a. Data Minimization

The central feature of the OOC proposal involves requiring controllers to collect the names of internet connected devices, and, if the device name includes the '0$S' prefix, treating the presence of the prefix as a request by the consumer to Opt Out.[27] However, this will in many cases require controllers to collect more personal data about consumers than they otherwise would – in particular, outside of the bluetooth/IoT context, many devices, apps, browsers, and websites do not currently collect device name. If accepted as a UOOM, the OOC proposal would require all controllers to pull this field, and would also require them to regularly ping devices for this information in order to detect whether the prefix has been added.

Relatedly, the OOC proposal will also result in device name being shared with additional third parties. If a controller (such as a mobile operating system) currently restricts access to device name to protect end-users' privacy, it may now need to make the field available to upstream services (*e.g.*, a mobile operating system would need to make device name available to all third-party apps).[28]

[26] Application § II.
[27] OOC Application at 3..
[28] *See* OOC Application at 7-9 (noting that both Android and Apple operating systems require special permissions to add the O$S prefix).

In addition, and particularly among NAI members who may only process pseudonymous identifiers such as browser or device IDs, any requirement to ingest and process device name introduces the risk of processing more sensitive types of personal data (such as a consumer's name – *e.g.* "Ralphie's iPhone," or street address – *e.g.* "123 Folsom St. WiFi"), which would be inconsistent with data minimization principles adhered to by many NAI members.[29] This is not a hypothetical risk, as NAI members have already learned from experience to be alert to the risk of personal data like names or clear email addresses appearing in URLs (*e.g.*, in cases when an email address is added as a parameter).

In addition, the applicant did not analyze what additional information may be made available to controllers that request user permission to access device name for the first time. It is not clear whether the platform permissions needed here are granular enough to be limited to *only* the device name, or if accessing device name would *also* require a broader category of permissions based on current operating permissions configurations. As it stands today, many app developers refrain from asking for too many device permissions because it impacts the user experience.

One potential solution would be to limit any requirement to read and honor the '0$S' prefix only to those controllers who already collect device name in the ordinary course of business; but the applicant did not address data minimization or consider such alternatives. Without further collaboration and consideration of data minimization issues, any requirement to collect and share new personal data in the form of device name is inconsistent with data minimization best practices.[30]

b. Implementation Issues

The OOC application does not adequately address the obligations that controllers (such as operating systems, browsers, devices, and apps) may have to pass user Opt Out signals to their upstream services, either by passing full device name or by otherwise communicating an Opt Out request. The OOC application does reference translating the '0$S' prefix at the device level into a GPC signal at the browser level, but it does not provide a clear set of criteria or requirements to achieve this goal in an effective, consistent manner for the benefit of controllers receiving a "translated" GPC signal.[31] The OOC application does provide some guidance to the effect that web browsers *may* look at the device name, and if the '0$S' prefix is present, set a GPC signal to '1.' But ,in general, the OOC application is too vague regarding the

[29] See Commentary to the NAI Code at 19 ("The NAI believes that it is appropriate for the Code to continue to encourage data minimization among its members for Tailored Advertising purposes").
[30] The CPA includes a duty of data minimization, which requires controllers to limit the collection of personal data to that which is "adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed." Colo. Rev. Stat. 6-1-1308(3). The Regulations further require controllers to "carefully consider each Processing purpose and determine the minimum Personal Data that is necessary, adequate, or relevant for the express purpose or purposes" of collection. Colo. Code Regs. § 904-3 Rule 6.07.
[31] *See* OOC Application at 4.

expectations of browsers and the websites accessed via those browsers when the device they are operating on has the '0$S' prefix. While some applications and connected devices (such as browsers, mobile apps, Bluetooth IoT devices, and WiFi-connected IoT devices) may have default permission to access device name, websites operating on a browser may not have these default permissions. The interaction between devices named with the '0$S' prefix on the one hand and browsers and websites operating on those devices on the other, as well as the interactions between two different candidate UOOMs (OOC and GPC), raise many potential complications that should be addressed in a way that adheres to the Collaboration Principle.

3. *The OOC Application does not Demonstrate Compliance with the Consumer Choice Principle.*

    a. The applicant does not provide any specific user interface for evaluation.

The OOC applicant has not demonstrated that the OOC proposal complies with the Consumer Choice Principle or the corresponding transparency requirements that UOOMs must meet in order to be included in the list of approved UOOMs.[32]

As we noted in our comments on the GPC application above, it is important to consider user interface as an integral part of any UOOM to ensure it satisfies the Consumer Choice Principle. However, the OOC application does not provide any of the information that would be needed to determine whether those user interface requirements have been met. In fact, the applicant states that "if, as we hope, the Colorado Department of Law decides to shortlist OptOutCode for consideration of a valid UOOM, Privacy4Cars plans to release a simple and free app for Consumers to be able to turn on and off OptOutCode (and test if OptOutCode is on or off)."[33]

This approach puts the cart before the horse – the DoL cannot properly evaluate whether OOC respects the Consumer Privacy Principle if it cannot examine the way a currently non-existent OOC application presents notice and choice to consumers, how default settings are handled, and so on. The applicant also notes that renaming a device with the '0$S' prefix "can be automated or semi-automated with code," which raises the issue of multiple implementations of OOC with different user interfaces.[34] Consistent with our recommendation for GPC, we recommend that any eventual recognition of OOC as a UOOM (which, as we detail above, would be premature at this point) be tied to specific implementations that the DoL can evaluate for compliance with the Consumer Choice Principle.

[32] *See* Colo. Code Regs. § 904-3 Rule 5.03(A) (2023) ("Platform, provider or developer of UOOM shall make clear (whether in its configuration or disclosure to the public) what the mechanism does (opt-out of the processing of personal data for sale, or targeted advertising, or both), whether the UOOM has been recognized by the CO Attorney General, and clearly describe applicable limitations").
[33] OOC Application at 7.
[34] *Id.* at 6.

b. The applicant does not adequately define the scope of consumer Opt-Out choices with regard to device names.

Apart from the user interface issues raised above, the OOC proposal also raises unique issues regarding the scope of consumer Opt Out requests interpreted through the '0$S' prefix. Specifically, use of a device-name prefix may trigger Opt Out requests that extend beyond the consumer who re-named her device seeking to Opt Out. For example, the OOC application indicates that controllers should read the name of the wifi router and various IoT devices that may be connected to the internet via the router, and if the prefix is present, treat it as the consumer's Opt Out request.[35] But if a consumer connect to a wifi network or IoT device owned or controlled by another person (such as a friend, family member, a business, or even a public wifi network), then this may cause a controller opt the consumer out, even if the consumer never made a request to opt out by re-naming her own device.

Allowing a business to opt all consumers out who connect to its wifi network by adding the '0$S' prefix to the name of its wifi router would be inconsistent with the purpose of the UOOM requirement, which is to empower *individual consumers* to manage how their data is collected and used. Another example to consider is when a consumer that owns a registered device (such as a smart TV) may have decided *not* to Opt Out using the '0$S' prefix, but another individual pairs a device with the TV that *does* include the prefix (such as a tablet using AirCast or a set of earbuds connected via Bluetooth). In that case, the OOC proposal does not include sufficient detail about how to ensure the controller collecting data via the TV and reading the Opt Out Signal from connected devices is respecting an authentic consumer Opt-Out choice.

In addition, the OOC application lacks clarity regarding what type of device name is eligible for the '0$S' prefix, as it could mean any of the following, each of which raises their own issues regarding who actually controls or owns them, as well as what specific controllers have permission to access the name (depending on where a controller sits in a data flow – *e.g.*, HTML/JavaScript code on a website, or an app installed on a device – the controller may not have access to all possible signals):

- Device name as discoverable on wifi
- Device name as discoverable on Bluetooth
- Service Set Identifier (SSID) of a connected wifi network

Controllers seeking to comply with UOOMs should not be expected to listen for and check all of these possible device names to make sure none are missed; instead, any approved UOOM relying on device name should be specific about what is covered.

Further, OptOutCode (as well as the CPA and Regulations) contemplates that a consumer may wish to override an Opt-Out choice made through a UOOM on a controller-by-controller basis; but OOC does not include a proposal for how that could be reflected accomplished[36] For example, the code examples provided by the applicant for Android and Apple iOS to read/write "device name" suggest that the absence of the '0$S' prefix on the current "device name" should

[35] *Id.* at 4.
[36] *See* OOC Application at 4-6; *see also* Colo. Code Regs. § 904-3 Rule 5.09 (consent after universal opt-out).

be interpreted as "*universal optout disabled*"; but actually, it is no signal at all and so remains ambiguous.[37]

C. Opt Out Machine

The NAI opposes recognizing Opt-Out Machine ("OOM") as a UOOM because OOM represents a market-based authorized agent service that is not apt for consideration as a UOOM.

The OOM application represents a proposal by the applicant, who offers a market-based authorized agent service that assists consumers in exercising their privacy rights, to require controllers to treat any consumer requests sent by its commercial service as a valid UOOM.[38] The NAI opposes including OOM as a valid UOOM because: (1) it represents a conceptual confusion between authorized agents and UOOMs; (2) it did not adhere to the Collaboration Principle; (3) it does not adhere to the Consumer Choice Principle; and (4) it does not provide for adequate information security.

1. *Authorized Agent Services are Not Appropriate Candidates for UOOMs because Controllers are Already Required to Honor Proper Authorized Agent Requests.*

The NAI recognizes that authorized agent services represent an important way for consumers to exercise their privacy rights, and that the CPA and the Regulations already require controllers to honor requests that consumers make through authorized agents (if applicable conditions are met), regardless of whether they are also listed as UOOMs.[39] However, an authorized agent is a distinct concept from a UOOM that presents different issues around consumer authorization and verification. As such, authorized agent services that are currently available in the market – including the applicant's – should not be approved as UOOMs, because doing so would result in confusion between the two distinct concepts and their requirements without any benefit to consumer privacy.

Specifically, the OOM application posits that requests sent by the OOM service via email should be recognized as a UOOM. However, this is duplicative of existing requirements under the CPA to honor valid authorized agent requests and therefore does not offer any additional benefits for consumer privacy. For example, email is already recognized by the Regulations as a method that controllers may be required to offer for consumers to submit requests, depending on how they interact with the controller.[40] Further, the NAI views the applicant as a specific market actor offering authorized agent services to submit requests on behalf of consumers that competes with other similar service providers; the applicant does not provide a specific user

[37] *See* OOC Application at 7-9.
[38] Opt Out Machine, Application for Inclusion in Colorado's UOOM Registry (hereinafter "OOM Application"), https://coag.gov/app/uploads/2023/11/Opt-Out-Machine-Application.pdf.
[39] The CPA requires controllers to comply with opt-out requests received from an authorized agent if the controller is able to authenticate, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf Colo. Rev. Stat. § 6-1-1306(1)(a)(II) (2023).
[40] Colo. Code Regs. § 904-3 Rule 4.02 (2023)

interface or signaling specification that could be made "universal" as a standard for submitting Opt Out requests. As such, its application for status as an UOOM is misconceived and fails to address the substantive requirements for valid authorized agents requests.

2. The OOM Application Did Not Honor the Collaboration Principle.

As discussed in more detail above and consistent with our comments on the OOC application, the OOM applicant did not honor the Collaboration Principle because it did not engage in a multi-stakeholder process as urged by the DoL. In addition, OOM appears to still be in the development phase, and so it would be premature to recognize it as a legally-binding UOOM.[41]

In any case, the NAI does not believe that a multi-stakeholder process would improve OOM's prospects as a UOOM because, as discussed above, it represents a confusion between authorized agents and UOOMs.

3. The OOM Application Does Not Comply With the Consumer Choice Principle.

The OOM Application does not include any examples of user interfaces employed by the OOM service, which makes it impossible to evaluate whether it complies with the Consumer Choice Principle when it determines what types of requests to communicate on behalf of consumers or to which controllers.

Further, the applicant's description of what OOM does exceeds the permitted scope for UOOMs,[42] as OOM appears to extend to customer rights beyond Opting Out, such as data access and deletion.[43] This raises the risk of automated and scaled email requests covering many consumer rights that may end up harming consumers without their knowledge or consent, such as permanently deleting their accounts across services and potentially making account information available to bad actors.

In addition the OOM application does not purport to limit its reach only to those controllers with whom the consumer intends to interact and submit Opt-Out requests, which is inconsistent with the Regulations.[44] Instead, OOM decides which controllers to reach out to and the application contains no information as to how it selects controllers to send requests to, whether consumers can indicate a preference as to which third parties they wish to exercise their right against, or whether OOM has the capability to automatically update consumer

[41] *See* OOM Application at 2 (stating that OOM "may in the future use Robotic Process Automation (bots, either traditional or AI powered) to automatically fill out forms, but this creates its own set of challenges[,]" indicating the development process is incomplete).

[42] The CPA and implementing rules limit UOOMs to opting out of targeted ads and sale of personal data. *See* Colo. Code Regs. § 904-3 5.02(A).

[43] *See* OOM Application at 6 (noting that the scope of OOMs functionality includes right to know request, right to delete requests, and right to correct request. These functions are allowed for authorized agents, but not UOOMs).

[44] *See* Colo. Code Regs. § 904-3 Rule 5.02(B).

preferences across websites, stating only that third parties would include data brokers.[45] Consequently, it would be difficult for a controller to determine that the request is legitimate. This would likely result in unfair disadvantage to certain controllers that are always included in email messages as determined by OOM (not by consumers), while others are excluded. This result is also inconsistent with the Regulations.[46]

Even if OOM were an apt candidate for a UOOM (and not, as it is in fact, merely a competitor in the market for authorized agent services), the OOM application is silent on the key issue of verifying that requests are user-enabled. Instead, the applicant simply states that user identity is verified by a "3rd party service provider" and the OOM simply notifies the controller that the user's identity has been verified.[47] This is deficient from the controller's perspective because the controller has no transparency into how the consumer interacted with the agent, can see no authorization of the agent, and has no insight into how the agent or its service provider have verified the consumer's identity or residency in the state of Colorado.

Instead, this appears to be an application to recognize OOM as a universally authorized agent. However, the CPA does not permit the DoL to mandate that controllers honor requests from certain agents. And regardless, OOM is an inadequate authorized agent because the application contains no process to allow controllers to authenticate the agent's authority to act on the consumer's behalf.[48] It mentions that only in "some cases" will it ask consumers for proof of identity. This presents the risk that OOM could choose to broadcast user email addresses requesting controllers to Opt a consumer Out even if OOM is not actually acting on behalf of the consumer (*i.e.* they are not actually user-authorized or user-enabled).

4. *The OOM application does not provide for adequate consumer authentication and security.*

Under the CPA, a UOOM must "permit the controller to accurately authenticate the consumer as a resident [of Colorado] and determine that the mechanism represents a legitimate request" to opt out of processing for targeted advertising and sale.[49] The OOM application states that in all cases, consumers will provide their physical address as a data matching tool, but only in some cases will consumers be asked to provide proof of identity. Under this description, OOM would not sufficiently allow for a controller to accurately confirm the identity and residency of the consumer.

The application also states that OOM collects significant personal data (including physical address, and sometimes proof of identity), but includes no details on how this information will

[45] *See* OOM Application at 3 (stating that OOM will reach out "proactively to likely holders of consumer data via email" without specifying how consumers can control who receives Opt Out requests and without reference to specific controllers the consumer has or will interact with).
[46] *See* Colo. Code Regs. § 904-3 Rule 5.06(E).
[47] *See* OOM Application at 3.
[48] *See* Colo. Code Regs. § 904-3 Rule 4.03(C).
[49] Colo. Rev. Stat. § 6-1-1313(2)(f) (2023).

be secured or used. This is an undue burden on the consumer, as alternative UOOMs (*e.g.*, the GPC) do not require such information. The Regulations require controllers to use reasonable data security measures when exchanging information in furtherance of data rights requests,[50] but the OOM application's stated method of email transmission does not use reasonable data security measures, because email is not a sufficiently secure mechanism to transmit personal data. In addition, the OOM application presents no discussion of how the OOM intends to protect against security risks the personal data it collects, stores, or transmits (such as encryption or access controls).

OOM is free to compete in the market for authorized agent services, but it is not an appropriate candidate for a UOOM. It is also striking that the other UOOM proposals (GPC and OOC) are open-source and free for consumers to use, yet OOM is expensive with prices that range up to $150.[51]

III. Conclusion

The NAI is supportive of the DoL's efforts to provide Colorado consumers with easy-to-use mechanisms enabling them to opt out of sale and targeting advertising, which is consistent with the NAI's mission and longstanding practice. However, as the DoL considers the applications for UOOMs represented in the shortlist, we urge careful consideration of the ability of each proposal to respect the Consumer Choice Principle by capturing the "affirmative, freely given, and unambiguous choice" of the user by including in the initial list of UOOMs not only the technical signal that may represent a consumer's choice to a controller but also the specific implementation of the opt-out mechanism through which consumers may exercise their choices.[52]

At this time, none of the proposals in the shortlist include necessary details about user interfaces or implementations that would allow the DoL to evaluate whether they are on by default or provide sufficient information to allow for an affirmative, freely given, and unambiguous choice, or if they represent authentic consumer choices and facilitate efficient adoption by businesses that avoids ambiguity and unnecessary or duplicative costs.[53]

In summary, for the reasons set forth above, the NAI recommends the following with respect to the candidate UOOMs included in the shortlist:

- **Global Privacy Control**: The NAI would support the inclusion in the initial list of approved UOOMs only implementations of GPC that demonstrably satisfy the Consumer Choice Principle and meet the requirements set forth in the CPA and the Regulations. The specification for the GPC itself, though, should not be included in the initial list independently of specific implementations.

[50] Colo. Code Regs. § 904-3 Rule 4.02 (2023).
[51] *See* OOM Application at 4.
[52] Colo. Rev. Stat. § 6-1-1313(2) (2023).
[53] *See generally* Colo. Code Regs. § 904-3 Rule 4.02 (regulations on default settings for universal opt-out mechanisms).

- **OptOutCode**: The NAI opposes the inclusion of OptOutCode in the initial list because the applicant did not go through the process of consulting with a broad base of stakeholders as urged by the OAG, which denied industry groups like the NAI the opportunity to provide meaningful input on its design and implementation. Further engagement with industry stakeholders, including the NAI, could strengthen a future submission of OptOutCode, as the list of UOOMs is intended to be updated "periodically."
- **Opt-Out Machine**: The NAI opposes the inclusion of the Opt-Out Machine in the initial list of UOOMs because the application represents a confusion between two distinct concepts in the CPA – that of a UOOM and that of an authorized agent.

Looking ahead, the NAI encourages the DoL to establish a formal process to provide for ongoing review of UOOMs, including an ongoing assessment of UOOMs already recognized as well as evaluation of new proposals, or new implementations of existing proposals. As highlighted in the shortlist of UOOM applications and these comments, the various signaling mechanisms, as well as implementations of these mechanisms, are continually evolving. Establishing a clear process for review, including opportunities for continued stakeholder input, would be a practical next step for the DoL to ensure that utilization of UOOMs across the marketplace are reviewed on a regular basis, and it would also provide for incentives for businesses developing and implementing UOOMs to plan ahead in their efforts to promote UOOMs that meet the established criteria.

Again, thank you for the work your office is conducting to ensure that signals being propagated by UOOMs represent authentic, freely given consumer choices and not default settings that represent interests other than a Colorado consumer's informed choice. If we can provide any additional information, or otherwise assist your office as it continues to engage in the process of developing a list of UOOMs, please do not hesitate to contact me at leigh@networkadvertising.org.

*****

Respectfully Submitted,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)

cc: Stevie DeGroff
Jill Szewczyk